


ArubaOS 6.4.2.1



Release Notes

Copyright Information

© 2014 Aruba Networks, Inc. Aruba Networks trademarks include  **airwave**, Aruba Networks®, Aruba Wireless Networks®, the registered Aruba the Mobile Edge Company logo, Aruba Mobility Management System®, Mobile Edge Architecture®, People Move. Networks Must Follow®, RFProtect®, Green Island®. All rights reserved. All other trademarks are the property of their respective owners.

Open Source Code

Certain Aruba products include Open Source software code developed by third parties, including software code subject to the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), or other Open Source Licenses. Includes software from Litech Systems Design. The IF-MAP client library copyright 2011 Infoblox, Inc. All rights reserved. This product includes software developed by Lars Fenneberg et al. The Open Source code used can be found at this site

http://www.arubanetworks.com/open_source

Legal Notice

The use of Aruba Networks, Inc. switching platforms and software, by all individuals or corporations, to terminate other vendors' VPN client devices constitutes complete acceptance of liability by that individual or corporation for this action and indemnifies, in full, Aruba Networks, Inc. from any and all legal actions that might be taken against it with respect to infringement of copyright on behalf of those vendors.

Warranty

This hardware product is protected by an Aruba warranty. For more information, refer to the ArubaCare service and support terms and conditions.

| | |
|---|-----------|
| Contents | 3 |
| Release Overview | 15 |
| Chapter Overview | 15 |
| Release Mapping | 15 |
| Supported Browsers | 16 |
| Contacting Support | 16 |
| Features in 6.4.x Releases | 17 |
| Features Introduced in ArubaOS 6.4.2.1 | 17 |
| AP Power Mode on AP-220 Series | 17 |
| In the CLI | 17 |
| Important Points to Remember | 18 |
| Features Introduced in ArubaOS 6.4.2.0 | 18 |
| AP-Platform | 18 |
| Support for the AP-210 Series | 18 |
| Enhanced Link Aggregation Support on AP-220 Series and AP-270 Series Access Points | 18 |
| Netgear AirCard 340U USB Modem Support | 18 |
| Netgear AirCard 341U USB Modem Support | 19 |
| VHT Support on AP-200 Series, AP-210 Series, AP-220 Series, and AP-270 Series Access Points | 19 |
| AP Regulatory | 19 |
| Channel 144 in Regulatory Domain Profile | 19 |
| Controller-Platform | 19 |
| Kernel Core Dump Enhancement | 19 |
| Web Content Classification | 19 |
| AP-Wireless | 20 |
| RTLS Station Message Frequency | 20 |

| | |
|---|----|
| Important Points to Remember | 20 |
| Video Multicast Rate Optimization | 20 |
| Features Introduced in ArubaOS 6.4.1.0 | 20 |
| AP-Platform | 20 |
| Support for AP-103H | 20 |
| Support for AP-200 Series | 21 |
| AP Regulatory | 21 |
| Downloadable Regulatory Table | 21 |
| Controller-Platform | 21 |
| 7000 Series Controllers | 21 |
| AirGroup | 22 |
| AP Fast Failover Support for Bridge-mode Virtual AP | 22 |
| DHCP Lease Limit on 7000 Series Controllers | 22 |
| Selective Multicast Stream | 22 |
| Security | 22 |
| Authentication Profile based User Idle Timeout | 22 |
| Global Firewall Parameters | 23 |
| Features Introduced in ArubaOS 6.4.0.2 | 23 |
| ArubaOS-AirWave Cross-Site Request Forgery Mitigation | 23 |
| Upgrade Recommendations | 23 |
| Fixed Software Versions | 23 |
| Frequently Asked Questions | 23 |
| EAP-MD5 Support | 24 |
| Features Introduced in ArubaOS 6.4.0.1 | 24 |
| PhoneHome Reporting Enhancements | 24 |
| Features Introduced in ArubaOS 6.4.0.0 | 24 |
| AP-Platform | 25 |
| Support for the AP-270 Series | 25 |
| Support for the AP-103 | 25 |

| | |
|--|----|
| Hotspot 2.0 | 25 |
| AP-220 Series Enhancements | 26 |
| AP-130 Series Functionality Improvements when Powered Over 802.3af (POE) | 26 |
| Franklin Wireless U770 4G Modem Support | 26 |
| Huawei E3276 LTE Modem Support | 26 |
| Authentication | 26 |
| Authentication Server Limits | 26 |
| EAP-MD5 Support | 26 |
| Controller-Platform | 27 |
| AirGroup | 27 |
| Default Behavior Changes | 27 |
| AirGroup DLNA UPnP Support | 27 |
| AirGroup mDNS Static Records | 27 |
| Group Based Device Sharing | 27 |
| AirGroup-WebUI Monitoring Dashboard Enhancements | 27 |
| AirGroup-Limitations | 28 |
| AppRF 2.0 | 28 |
| Policy Configuration | 28 |
| Bandwidth Contract Configuration | 29 |
| Global Bandwidth Contract Configuration | 29 |
| AppRF Dashboard Application Visibility | 29 |
| Branch | 29 |
| Centralized BID Allocation | 29 |
| Controller LLDP Support | 30 |
| High Availability | 30 |
| High Availability Configuration Using the WebUI | 30 |
| Client State Synchronization | 30 |
| High Availability Inter-controller Heartbeats | 31 |
| Extended Standby Controller Capacity | 31 |
| Features not Supported on 600 Series Controllers | 31 |

| | |
|---|-----------|
| Control Plane Bandwidth Contracts Values | 32 |
| Automatic GRE from IAP | 32 |
| DHCP Lease Limit | 32 |
| IPv6 | 32 |
| Multicast Listener Discovery (MLDv2) Snooping | 32 |
| Source Specific Multicast | 32 |
| Dynamic Multicast Optimization | 33 |
| Understanding MLDv2 Limitations | 33 |
| Static IPv6 GRE Tunnel Support | 33 |
| Important Points to Remember | 33 |
| Understanding Static IPv6 GRE Tunnel Limitations | 33 |
| IGMPv3 Support | 33 |
| IPv6 Enhancements | 34 |
| VRRPv3 Support on Controllers | 34 |
| Understanding VRRP Limitations | 34 |
| Security | 34 |
| Palo Alto Networks Firewall Integration | 34 |
| Application Single Sign-On Using L2 Network Information | 34 |
| 802.11w Support | 35 |
| Ability to Disable Factory-Default IKE/IPsec Profiles | 35 |
| AOS/ClearPass Guest Login URL Hash | 35 |
| Authentication Server Load Balancing | 35 |
| Enhancements in the User Authentication Failure Traps | 35 |
| RADIUS Accounting on Multiple Servers | 35 |
| RADIUS Accounting for VIA and VPN Users | 35 |
| Spectrum Analysis | 35 |
| AP Platform Support for Spectrum Analysis | 35 |
| Voice and Video | 36 |
| Unified Communication and Collaboration | 36 |

| | |
|---|-----------|
| AP Support | 36 |
| MIB and Trap Enhancements | 36 |
| Modified Traps | 36 |
| Regulatory Updates | 39 |
| Regulatory Updates in ArubaOS 6.4.2.1 | 39 |
| Regulatory Updates in ArubaOS 6.4.2.0 | 40 |
| Regulatory Updates in ArubaOS 6.4.0.2 | 43 |
| Regulatory Updates in ArubaOS 6.4.0.0 | 44 |
| Resolved Issues | 47 |
| Resolved Issues in ArubaOS 6.4.2.1 | 47 |
| Activate | 47 |
| Airgroup | 47 |
| Air Management-IDS | 47 |
| AP-Platform | 48 |
| AP-Wireless | 48 |
| Base OS Security | 49 |
| Configuration | 49 |
| Controller-Datapath | 50 |
| Controller-Platform | 50 |
| HA-Lite | 51 |
| Hotspot-11u | 51 |
| Local Database | 51 |
| Mobility | 51 |
| Station Management | 52 |
| VRRP | 52 |
| WebUI | 53 |
| Resolved Issues in ArubaOS 6.4.2.0 | 53 |
| 802.1X | 53 |

| | |
|--|--------------------|
| Air Management-IDS | 53 |
| AP-Platform | 54 |
| AP-Wireless | 54 |
| ARM | 54 |
| Authentication | 54 |
| Base OS Security | 55 |
| Controller-Datapath | 55 |
| Controller-Platform | 56 |
| GRE | 56 |
| Licensing | 56 |
| LLDP | 57 |
| QoS | 57 |
| Remote AP | 57 |
| Role/VLAN Derivation | 58 |
| Station Management | 58 |
| WebUI | 58 |
| Resolved Issues in ArubaOS 6.4.1.0 | 58 |
| AirGroup | 59 |
| Air Management-IDS | 59 |
| AP Regulatory | 60 |
| AP-Platform | 60 |
| AP-Wireless | 61 |
| ARM | 62 |
| Authentication | 62 |
| Base OS Security | 62 |
| Captive Portal | 63 |
| Certificate Manager | 63 |
| Configuration | 63 |
| Controller-Datapath | 64 |

| | |
|--|--------------------|
| Controller-Platform | 65 |
| DHCP | 66 |
| LLDP | 66 |
| Local Database | 67 |
| IPsec | 67 |
| Master-Redundancy | 67 |
| RADIUS | 68 |
| Remote AP | 68 |
| Role/VLAN Derivation | 69 |
| Routing | 69 |
| Startup Wizard | 70 |
| Station Management | 70 |
| Voice | 70 |
| WebUI | 71 |
| XML API | 72 |
| Resolved Issues in ArubaOS 6.4.0.3 | 72 |
| Base OS Security | 72 |
| Resolved Issues in ArubaOS 6.4.0.2 | 72 |
| AirGroup | 72 |
| Application Monitoring (AMON) | 73 |
| AP-Platform | 73 |
| AP-Regulatory | 73 |
| AP-Wireless | 74 |
| Authentication | 74 |
| Base OS Security | 74 |
| Captive Portal | 75 |
| Controller-Datapath | 75 |
| Controller-Platform | 75 |
| IPSec | 75 |

| | |
|--|----|
| Mobility | 76 |
| RADIUS | 76 |
| Remote AP | 76 |
| Station Management | 76 |
| Voice | 77 |
| WebUI | 77 |
| Resolved Issues in ArubaOS 6.4.0.1 | 77 |
| PhoneHome | 77 |
| Resolved Issues in ArubaOS 6.4.0.0 | 77 |
| 802.1X | 78 |
| AirGroup | 78 |
| Air Management-IDS | 78 |
| AP-Datapath | 79 |
| AP-Platform | 79 |
| AP Regulatory | 82 |
| AP-Wireless | 83 |
| ARM | 87 |
| Authentication | 87 |
| Base OS Security | 87 |
| Configuration | 90 |
| Captive Portal | 90 |
| Controller-Datapath | 91 |
| Controller-Platform | 94 |
| Control Plane Security | 96 |
| DHCP | 96 |
| Generic Routing Encapsulation | 96 |
| GSM | 96 |
| Guest Provisioning | 97 |
| HA-Lite | 97 |

| | |
|---|------------|
| Hardware Management | 97 |
| IGMP Snooping | 97 |
| IPv6 | 98 |
| Licensing | 98 |
| Local Database | 98 |
| Master-Redundancy | 98 |
| Mesh | 99 |
| Mobility | 99 |
| PPPoE | 99 |
| Remote AP | 100 |
| Role/VLAN Derivation | 101 |
| SNMP | 101 |
| Station Management | 102 |
| TACACS | 102 |
| VLAN | 102 |
| Voice | 103 |
| WebUI | 104 |
| WLAN Management System | 105 |
| XML API | 106 |
| Known Issues and Limitations | 107 |
| Known Issues and Limitations in ArubaOS 6.4.2.1 | 107 |
| Airgroup | 107 |
| AP-Platform | 107 |
| AP-Regulatory | 107 |
| AP Wireless | 108 |
| Controller-Datapath | 108 |
| Controller-Platform | 109 |
| HA-Lite | 109 |

| | |
|---|-----|
| Local Database | 109 |
| LLDP | 109 |
| Mobility | 110 |
| Remote AP | 110 |
| Voice | 110 |
| WebUI | 110 |
| Wi-Fi Multimedia | 111 |
| Known Issues and Limitations in ArubaOS 6.4.2.0 | 111 |
| AP Wireless | 111 |
| AP Platform | 111 |
| Controller-Datapath | 112 |
| Policy Based Routing | 112 |
| WebCC | 112 |
| Known Issues and Limitations in ArubaOS 6.4.1.0 | 112 |
| AP Regulatory | 112 |
| Controller-Datapath | 113 |
| Remote AP | 113 |
| WebUI | 113 |
| Known Issues and Limitations in ArubaOS 6.4.0.2 | 114 |
| AP-Wireless | 114 |
| Base OS Security | 114 |
| Controller-Datapath | 114 |
| Controller-Platform | 115 |
| LLDP | 115 |
| PhoneHome | 115 |
| Startup Wizard | 115 |
| Known Issues and Limitations in ArubaOS 6.4.0.1 | 116 |
| PhoneHome | 116 |
| Known Issues and Limitations in ArubaOS 6.4.0.0 | 116 |

| | |
|--|------------|
| AirGroup | 116 |
| AP-Platform | 117 |
| AP-Wireless | 117 |
| Base OS Security | 118 |
| Captive Portal | 118 |
| Configuration | 119 |
| Controller-Datapath | 119 |
| Controller-Platform | 120 |
| DHCP | 121 |
| Hardware-Management | 121 |
| IPSec | 122 |
| Local Database | 122 |
| LLDP | 122 |
| Master-Local | 123 |
| RADIUS | 123 |
| Remote AP | 123 |
| Station Management | 124 |
| Voice | 124 |
| WebUI | 125 |
| Issues Under Investigation | 125 |
| AP-Wireless | 125 |
| Controller-Datapath | 125 |
| Controller-Platform | 126 |
| Upgrade Procedure | 127 |
| Upgrade Caveats | 127 |
| Peer Controller Upgrade Requirement | 128 |
| Points to Remember | 128 |
| Installing the FIPS Version of ArubaOS 6.4.2.1 | 128 |

| | |
|---|-----|
| Before Installing FIPS Software | 128 |
| Important Points to Remember and Best Practices | 129 |
| Memory Requirements | 129 |
| Backing up Critical Data | 130 |
| Backup and Restore Compact Flash in the WebUI | 130 |
| Backup and Restore Compact Flash in the CLI | 130 |
| Upgrading in a Multi-Controller Network | 131 |
| Upgrading to ArubaOS 6.4.2.1 | 131 |
| Install Using the WebUI | 131 |
| Upgrading From an Older version of ArubaOS | 131 |
| Upgrading From a Recent version of ArubaOS | 132 |
| Install Using the CLI | 133 |
| Upgrading From an Older Version of ArubaOS | 133 |
| Upgrading From a Recent Version of ArubaOS | 133 |
| Downgrading | 135 |
| Before You Begin | 135 |
| Downgrading Using the WebUI | 136 |
| Downgrading Using the CLI | 136 |
| Before You Call Technical Support | 137 |

ArubaOS 6.4.2.1 is a software patch release that introduces fixes to the issues identified in previous releases and some software enhancements.



See the [Upgrade Procedure on page 127](#) for instructions on how to upgrade your controller to this release.

Chapter Overview

- [Features in 6.4.x Releases on page 17](#) provides a description of features and enhancements introduced in ArubaOS 6.4.x release versions.
- [Regulatory Updates on page 39](#) describes the regulatory updates in ArubaOS 6.4.x release versions.
- [Resolved Issues on page 47](#) describes the issues resolved in ArubaOS 6.4.x release versions.
- [Known Issues and Limitations on page 107](#) describes the known and outstanding issues identified in previous ArubaOS 6.4.x release versions.
- [Upgrade Procedure on page 127](#) describes the procedures for upgrading a controller to ArubaOS 6.4.2.1.

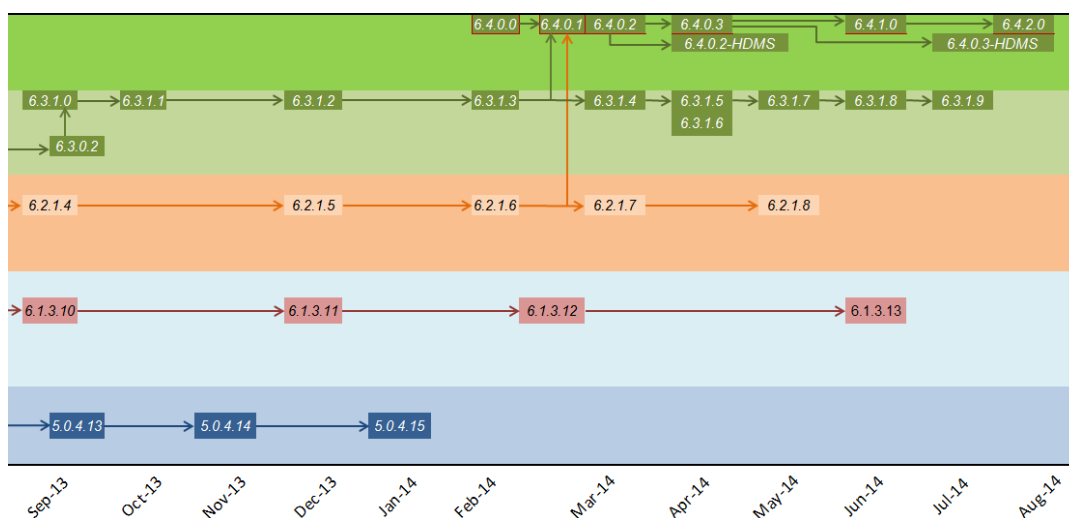
Release Mapping

This version of ArubaOS is based off of the ArubaOS 6.4.2.0 release. This version of ArubaOS includes features and bug fixes from the following releases:

- 6.4.2.0 and all earlier 6.4.x.x releases.
- 6.3.1.10 and all earlier 6.3.x.x releases
- 6.2.1.8 and all earlier 6.2.x.x releases
- 6.1.3.13 and all earlier 6.1.x.x and 6.0.x.x releases
- 5.0.4.16 and all earlier 5.0.x.x releases

The following illustration shows the patch and maintenance releases that are included in their entirety in ArubaOS 6.4.2.0:

Figure 1 ArubaOS Releases and Code Stream Integration



Supported Browsers

The following browsers are officially supported for use with ArubaOS 6.4.2.1 WebUI:

- Microsoft Internet Explorer 10.x and 11 on Windows 7 and Windows 8
- Mozilla Firefox 23 or higher on Windows Vista, Windows 7, and MacOS
- Apple Safari 5.1.7 or higher on MacOS

Contacting Support

Table 1: *Contact Information*

| | |
|---|---|
| Main Site | arubanetworks.com |
| Support Site | support.arubanetworks.com |
| Airheads Social Forums and Knowledge Base | community.arubanetworks.com |
| North American Telephone | 1-800-943-4526 (Toll Free) 1-408-754-1200 |
| International Telephone | http://www.arubanetworks.com/support-services/support-program/contact-support/ |
| Software Licensing Site | https://licensing.arubanetworks.com/ |
| End of Support Information | http://www.arubanetworks.com/support-services/end-of-life-products/end-of-life-policy/ |
| Security Incident Response Team (SIRT) | http://www.arubanetworks.com/support-services/security-bulletins/ |
| Support Email Addresses | |
| Americas, EMEA, and APAC | support@arubanetworks.com |
| Security Incident Response Team (SIRT) | sirt@arubanetworks.com |

This chapter describes features introduced in ArubaOS 6.4.x release versions. For more information about features introduced in ArubaOS 6.4.x, refer to the *ArubaOS 6.4.x User Guide*.

Features Introduced in ArubaOS 6.4.2.1

This section describes the new features and enhancements introduced in ArubaOS 6.4.2.1.

AP Power Mode on AP-220 Series

Starting with ArubaOS 6.4.2.1, a new configuration parameter **ap-poe-power-optimization** is introduced. This parameter is available under the **ap provisioning-profile** command. When this parameter is set to **enabled**, the controller disables the USB and the Ethernet (eth1) ports of AP-220 Series access points. Once the ports are disabled, the AP runs in reduced power mode.



Overriding the AP power mode sets the maximum power request for LLDP TLV to 17.1W instead of 19.0W.

In the CLI

Use the following commands to configure an AP to run in reduced power mode using the CLI:

```
(host) (config) #ap provisioning-profile default
(host) (Provisioning profile "default") #ap-poe-power-optimization enabled
```

Use the following command to verify the configuration using the CLI:

```
(host) (config) #show ap provisioning-profile default
```

```
Provisioning profile "default"
```

| Parameter | Value |
|---|-------|
| Remote-AP | No |
| Master IP/FQDN | N/A |
| PPPOE User Name | N/A |
| PPPOE Password | N/A |
| PPPOE Service Name | N/A |
| USB User Name | N/A |
| USB Password | N/A |
| USB Device Type | none |
| USB Device Identifier | N/A |
| USB Dial String | N/A |
| USB Initialization String | N/A |
| USB TTY device data path | N/A |
| USB TTY device control path | N/A |
| USB modeswitch parameters | N/A |
| Link Priority Ethernet | 0 |
| Link Priority Cellular | 0 |
| Cellular modem network preference | auto |
| Username of AP so that AP can authenticate to 802.1x using PEAP | N/A |
| Password of AP so that AP can authenticate to 802.1x using PEAP | N/A |
| Uplink VLAN | 0 |
| USB power mode | auto |

Important Points to Remember

- By default, the AP operates in normal mode with the USB and Ethernet ports enabled.
- Changing the **ap-poe-power-optimization** parameter requires a reboot of the AP.
- In case the AP has an external DC power source, the USB and Ethernet (eth1) ports are not disabled even after setting the **ap-poe-power-optimization** to **enabled**.

Features Introduced in ArubaOS 6.4.2.0

This section describes the new features and enhancements introduced in ArubaOS 6.4.2.0.

AP-Platform

Support for the AP-210 Series

The Aruba AP-210 Series (AP-214 and AP-215) wireless access points support the IEEE 802.11ac standard for high-performance WLAN. These access points use MIMO (Multiple-Input, Multiple-Output) technology and other high-throughput mode techniques to deliver high-performance, 802.11ac 2.4 GHz and 802.11ac 5 GHz functionality while simultaneously supporting existing 802.11a/b/g wireless services. The AP-210 Series access points work only in conjunction with an Aruba Controller. The Aruba AP-210 Series access point provides the following capabilities:

- Wireless transceiver
- Protocol-independent networking functionality
- IEEE 802.11a/b/g/n/ac operation as a wireless access point
- IEEE 802.11a/b/g/n/ac operation as a wireless air monitor
- Compatibility with IEEE 802.3at PoE+ and 802.3af PoE
- Central management configuration and upgrades through a controller

For more information, see the *AP-210 Series Wireless Access Point Installation Guide*.

Enhanced Link Aggregation Support on AP-220 Series and AP-270 Series Access Points

The AP-220 Series (AP-224 and AP-225) and AP-270 Series (AP-274 and AP-275) wireless access points support link aggregation using either standard port-channel (configuration based) or Link Aggregation Control Protocol (protocol signaling based). These access points can optionally be deployed with LACP configuration to benefit from the higher (greater than 1 Gbps) aggregate throughput capabilities of the two radios.

ArubaOS 6.4.2.0 introduces the **AP LACP LMS map information** profile, a local profile that maps a LMS IP address to a GRE striping IP address. If the AP fails over to a standby or backup controller, the AP LACP LMS map information profile on the new controller defines the IP address that AP uses to terminate 802.11g radio tunnels on the new controller. This feature allows AP-220 Series or AP-270 Series access points to form a 802.11g radio tunnel to a backup controller the event of a controller failover, even if the backup controller is in a different L3 network. In previous releases, the GRE striping IP address was defined in the global AP system profile, which did not allow APs to maintain GRE striping tunnels if the AP failed over to a backup controller in a different L3 network. The GRE striping IP address parameter is deprecated from the AP system profile in ArubaOS 6.4.2.0.

Netgear AirCard 340U USB Modem Support

ArubaOS 6.4.2.0 introduces support of the Netgear AirCard 340U USB modem for AT&T's LTE service on the RAP-3WN, RAP-108, RAP-109, and RAP-155.

Netgear AirCard 341U USB Modem Support

ArubaOS 6.4.2.0 introduces support of the Netgear AirCard 341U USB modem for Sprint's LTE service on the RAP-3WN, RAP-108, RAP-109, and RAP-155.

VHT Support on AP-200 Series, AP-210 Series, AP-220 Series, and AP-270 Series Access Points

This feature enables Very High Throughput (VHT) rates on the 2.4 GHz band, providing 256-QAM modulation and encoding that allows for 600 Mbit/sec performance over 802.11n networks. Maximum data rates are increased on the 2.4 GHz band through the addition of VHT Modulation and Coding Scheme (MCS) values 8 and 9, which support the highly efficient modulation rates in 256-QAM. Starting with ArubaOS 6.4.2.0, VHT is supported on AP-200 Series (AP-204 and AP-205), AP-210 Series (AP-214 and AP-215), AP-220 Series (AP-224 and AP-225), and AP-270 Series (AP-274 and AP-275) wireless access points on both 20 MHz and 40 MHz channels.

Using the controller CLI or WebUI, VHT MCS values 0-9 are enabled, overriding the existing high-throughput (HT) MCS values 0-7, which have a lower maximum data rate. However, this feature should be disabled if individual rate selection is required.

AP Regulatory

Channel 144 in Regulatory Domain Profile

If Dynamic Frequency Selection (DFS) channel is enabled in FCC, an AP can use channel 144 as primary or secondary channel. However, most clients do not support channel 144. Hence when enabling DFS channel in FCC:

- If the deployment is 20 MHz mode, do not use channel 144 in regulatory domain profile.
- If the deployment is 40 MHz mode, do not use channel 140-144 in regulatory domain profile.
- If the deployment is 80 MHz mode, do not use channel 132-144 in regulatory domain profile.

This is because most older clients do not support channel 144, even though they support DFS channel. An AP in 80 MHz or 40 MHz mode chooses:

- Channel 144 as the primary channel – Here, most clients do not connect to the AP.
- Channel 140 as the primary channel and channel 144 as secondary channel – Here, most 802.11n clients do not connect to the AP over 40 MHz.

Controller-Platform

Kernel Core Dump Enhancement

Starting with ArubaOS 6.4.2.0, a new command **kernel coredump** is introduced. This command enables the controller to capture the snapshot of the working memory of the control plane when the control plane has terminated abnormally. After issuing this command, you may run the **write memory** command to save the configuration. This will enable the kernel core dumps across reboots.

Web Content Classification



This feature is available for all customers with a PEF license to use during an early preview period. Eventually, Aruba intends to license this feature as an annual subscription. License enforcement timeline and pricing information will be made available once the SKUs and prices are finalized.

Currently, the AppRF feature displays summary of all traffic in the controller. But a large amount of traffic on the controller is from the web, hence this release of ArubaOS introduces the implementation of the Web

Content Classification (WebCC) feature. When the WebCC feature is enabled, all web traffic (http and https) is classified. The classification is done in data path as the traffic flows through the controller.

This feature is supported on all 7xxx controllers.

The current policy enforcement model relies on L3/L4 information of the packet or L7 information with Deep Packet Inspection (DPI) support to apply rules. WebCC complements this as the user is allowed to apply firewall policies based on web content category and reputation.

Benefits of WebCC:

1. Prevention of malicious malware, spyware, or adware by blocking known dangerous websites
2. Visibility into web content category-level
3. Visibility into web sites accessed by the user

AP-Wireless

RTLS Station Message Frequency

Currently, when configuring the RTLS server under **ap system-profile**, the valid range of values for **station-message-frequency** was 5-3600 seconds. There are deployments that may require this to be configurable to as frequently as 1 per second. Starting with ArubaOS 6.4.2.0, you can set the **station-message-frequency** parameter in the 1-3600 seconds range. Setting the frequency to 1 means a report would be sent for every station every second. A value of 5 would mean that a report for any particular station would be sent at 5 second intervals.

Important Points to Remember

- Sending more frequent reports to the server can improve the accuracy of the location calculation.
- Configuring an AP to send reports more frequently adds additional load in terms of CPU usage.

Video Multicast Rate Optimization

The **Multicast Rate** parameter is renamed to **Video Multicast Rate Optimization**.

The **Video Multicast Rate Optimization** parameter overrides the configuration of the **BC/MC Rate Optimization** parameter for VI-tagged multicast traffic.

Features Introduced in ArubaOS 6.4.1.0

This section describes the new features and enhancements introduced in ArubaOS 6.4.1.0.

AP-Platform

Support for AP-103H

The Aruba AP-103H wireless access point supports the IEEE 802.11n standard for high-performance WLAN. It is a dual radio, 2x2:2 802.11n access point. This access point uses MIMO (Multiple-Input, Multiple-Output) technology and other high-throughput mode techniques to deliver high-performance 802.11n 2.4 GHz or 5 GHz functionality while simultaneously supporting existing 802.11a/b/g wireless services. AP-103H is equipped with a total of three active Ethernet ports (ENET 0-2). It is a wall-box type access point. The AP-103H access point works only with an Aruba controller.

The Aruba AP-103H access point provides the following capabilities:

- Wireless transceiver
- Protocol-independent networking functionality
- IEEE 802.11a/b/g/n operation as a wireless access point

- IEEE 802.11 a/b/g/n operation as a wireless air monitor
- Compatibility with IEEE 802.3af PoE
- Central management configuration and upgrades through a controller

For more information, see the *Aruba AP-103H Wireless Access Point Installation Guide*.

Support for AP-200 Series

The Aruba AP-200 Series (AP-204 and AP-205) wireless access points support the IEEE 802.11 ac and 802.11 n standards for high-performance WLAN. It is a dual radio, 2x2:2 802.11 ac access point. These access points use MIMO (Multiple-Input, Multiple-Output) technology and other high-throughput mode techniques to deliver high-performance, 802.11 n 2.4 GHz and 802.11 ac 5 GHz functionality while simultaneously supporting legacy 802.11 a/b/g wireless services.

The Aruba AP-200 Series access point provides the following capabilities:

- Wireless transceiver
- Protocol-independent networking functionality
- IEEE 802.11 a/b/g/n/ac operation as a wireless access point
- IEEE 802.11 a/b/g/n/ac operation as a wireless air monitor
- Compatibility with IEEE 802.3af PoE
- Central management configuration and upgrades through a controller

For more information, see the *Aruba AP-200 Series Wireless Access Point Installation Guide*.

AP Regulatory

Downloadable Regulatory Table

The downloadable regulatory table features allows new regulatory approvals to be distributed without waiting for a new software patch and upgrade. A separate file, called the Regulatory-Cert, containing AP regulatory information will be released periodically on the customer support site. The Regulatory-Cert file can then be uploaded to the Aruba controller and pushed to deployed APs.

Controller-Platform

7000 Series Controllers

The Aruba 7000 Series controllers is an integrated controller platform. The platform acts as a software services platform targeting small to medium branch offices and enterprise networks.

The 7000 Series controllers include three models that provide varying levels of scalability.

Table 2: *Aruba 7000 Series Controllers*

| Model | Number of APs Supported | Number of Users Supported |
|-------|-------------------------|---------------------------|
| 7005 | 16 | 1024 |
| 7010 | 32 | 2048 |
| 7030 | 64 | 4096 |

For more information, see the installation guide for each controller model.

AirGroup

The following AirGroup service changes are effective in ArubaOS 6.4.1.0:

- The **Chromecast** service is renamed to **DIAL**.
- The **googlecast** service is introduced.

AP Fast Failover Support for Bridge-mode Virtual AP

High Availability (HA) support for bridge mode in Campus AP is introduced in ArubaOS 6.4.1.0. In previous versions of ArubaOS the fast failover feature for Campus AP was supported using tunnel or decrypt mode. Now support has been extended to bridge mode as well.



AP Fast Failover on bridge forwarding mode virtual AP is supported on 7200 Series controllers only.

DHCP Lease Limit on 7000 Series Controllers

The following table outlines the maximum number of DHCP leases supported on the new 7000 Series controllers.

Table 3: *DHCP Lease Limit*

| Platform | DHCP Lease Limit |
|----------|------------------|
| 7005 | 512 |
| 7010 | 1024 |
| 7030 | 2048 |

Selective Multicast Stream

The selective multicast group is based only on the packets learned through Internet Group Management Protocol (IGMP).

- When **broadcast-filter all** parameter is enabled, the controller would allow multicast packets to be forwarded only if the following conditions are met:
 - packets originating from the wired side have a destination address range of 225.0.0.0 - 239.255.255.255
 - a station has subscribed to a multicast group.
- When IGMP snooping/proxy is disabled, the controller is not aware of the IGMP membership and drops the multicast flow.
- If Dynamic Multicast Optimization (DMO) is enabled, the packets are sent with 802.11 unicast header.
- If AirGroup is enabled, mDNS (SSDP) packets are sent to the AirGroup application. The common address for mDNS is 224.0.0.251 and SSDP is 239.255.255.250.

Security

Authentication Profile based User Idle Timeout

Starting with ArubaOS 6.4.1.0, the **user-idle-timeout** parameter under AAA profile accepts a value of 0. Entering a value of 0, L3 user state is removed immediately upon disassociation. In other words, the controller deletes the user immediately after disassociation or disconnection from the wireless network. If RADIUS accounting is configured, the controller sends an accounting STOP message to the RADIUS server.



User idle timeout of 0 should not be configured for wired, split-tunnel, VIA, and VPN users. It is applicable only for wireless users in tunnel and decrypt-tunnel forwarding modes.

Global Firewall Parameters



This feature works only when L3 user entry exists on the controller.

Starting with ArubaOS 6.4.1.0, Address Resolution Protocol (ARP) and Gratuitous ARP packets from wired and wireless clients can be monitored or policed beyond a configured threshold value. The following new parameters are introduced as part of the global firewall parameters:

- **Monitor/police ARP attack**
- **Monitor/police Gratuitous ARP attack**

Additional options to drop excessive packets or blacklist a client is introduced.



Blacklisting of wired clients is not supported.

Features Introduced in ArubaOS 6.4.0.2

This section describes the new features introduced in ArubaOS 6.4.0.2.

ArubaOS-AirWave Cross-Site Request Forgery Mitigation

To defend against Cross-Site Request Forgery (CSRF) attacks, an enhancement is added to use randomly generated session-ID in HTTP transactions with the ArubaOS WebUI. As a consequence, AirWave must be upgraded to AirWave 7.7.10 so that it includes the session-ID in its requests.

Upgrade Recommendations

- Upgrade to AirWave 7.7.10 to maintain full functionality.
- Upgrade controllers to ArubaOS 6.4.0.2 to mitigate CSRF. Controllers that are not upgraded will continue to work with the upgraded AirWave 7.7.10 as controllers with older ArubaOS software image ignore the session-ID in the request.

Fixed Software Versions

- ArubaOS 6.4.0.2
- AirWave 7.7.10

Frequently Asked Questions

Q. What happens if I upgrade ArubaOS but not AirWave?

A. If you upgrade the controller to ArubaOS 6.4.0.2, AirWave must also be upgraded to version 7.7.10 to maintain full functionality. If AirWave 7.7.10 patch is not applied, client monitoring, AppRF information, and push certificate will not work on the controller with ArubaOS 6.4.0.2 software image.

Q. What happens if I upgrade to AirWave 7.7.10 but not all controllers to ArubaOS 6.4.0.2?

A. If you upgrade to AirWave 7.7.10, controllers that are not upgraded to ArubaOS 6.4.0.2 will continue to work with the upgraded AirWave 7.7.10, but will ignore the session-ID in the request.

Q. Where can I find more information on CSRF?

A. http://en.wikipedia.org/wiki/Cross-site_request_forgery

EAP-MD5 Support

The controller does not support EAP-MD5 authentication for wireless clients. In ArubaOS 6.3.x and ArubaOS 6.4, EAP-MD5 authentication for wired clients failed. This issue is fixed in ArubaOS 6.4.0.2.

Features Introduced in ArubaOS 6.4.0.1

This section describes the new features introduced in ArubaOS 6.4.0.1.

PhoneHome Reporting Enhancements

The PhoneHome feature can be enabled by selecting the **Enable** option under **Maintenance > File > Aruba TAC Server** section of the WebUI. When Auto PhoneHome is enabled, the first report occurs 7 days after the feature has been enabled. The Auto PhoneHome Report is disabled by default.



The PhoneHome feature does not report any user information including client MAC address or user names.

The PhoneHome feature, allows a controller to proactively report events such as hardware failures, software malfunctions and other critical events. When PhoneHome is enabled on a controller, the customer support portal will provide a summary of deployed APs and licenses that are linked to a specific controller. To view this information, you must enter a valid email address with a domain name associated with your controller in the **Maintenance > File > Aruba TAC Server** section of the controller WebUI. Access to this information also requires an active support contract and login access to the customer portal.

Previously, PhoneHome required reports to be sent over SMTP. However, starting with ArubaOS 6.4, controllers have the option to send PhoneHome reports over HTTPS to the Aruba Activate server.

If your controller is behind the proxy server and does not have direct access to the Internet, you can configure PhoneHome to send reports using an SMTP server. PhoneHome integration with Activate offers following benefits:

- **Simpler configuration**—PhoneHome only requires you to configure the email ID of the network administrator managing the device, as Activate already has information to accurately identify your controller. This email address appears in the output of the command.
- **Smaller bandwidth requirements**—When the PhoneHome feature sends the report to the Activate server, the PhoneHome report is zipped into a smaller package, then divided into smaller 1 MB pieces before being sent to the server using secure HTTPS. Only reports sent to Activate are zipped before they are sent, so reports sent to Activate use less bandwidth than a report sent to a SMTP server.
- **Enhanced error management**—If any individual portion of the report is not successfully received by the Activate server, PhoneHome makes up to three attempts to resend just that portion of the file, rather than resending the entire report. Reports sent via SMTP must be resent in their entirety if any portion is not received by the SMTP server.
- **Automatic removal of old reports**—Once the entire report is sent to the Activate server, Activate sends an acknowledgment to the controller, prompting the controller to delete its local copy of the report.
- The PhoneHome feature can be enabled or disabled using the **Maintenance > File > Aruba TAC Server** option in the WebUI. The same can also be done through **phonehome [enable | disable]** option in the CLI.

Features Introduced in ArubaOS 6.4.0.0

This section describes the new features introduced in ArubaOS 6.4.0.0.

AP-Platform

Support for the AP-270 Series

The Aruba AP-270 Series (AP-274 and AP-275) wireless access points are environmentally hardened, outdoor rated, dual-radio IEEE 802.11ac wireless access points. These access points use MIMO (Multiple-Input, Multiple-Output) technology and other high-throughput mode techniques to deliver high-performance, 802.11ac 2.4 GHz and 5 GHz functionality while simultaneously supporting existing 802.11a/b/g/n wireless services.

Support for the AP-103

The Aruba AP-103 wireless access point supports the IEEE 802.11n standard for high-performance WLAN. This access point uses MIMO (Multiple-Input, Multiple-Output) technology and other high-throughput mode techniques to deliver high performance, 802.11n 2.4 GHz or 5 GHz functionality while simultaneously supporting existing 802.11a/b/g wireless services.

Hotspot 2.0

Hotspot 2.0 is a Wi-Fi Alliance Passpoint specification based upon the 802.11u protocol that provides wireless clients with a streamlined mechanism to discover and authenticate to suitable networks, and allows mobile users the ability to roam between partner networks without additional authentication.

ArubaOS 6.4 supports Hotspot 2.0 with enhanced network discovery and selection. Clients can receive general information about the network identity, venue and type via management frames from the Aruba AP. Clients can also query APs for information about the network's available IP address type (IPv4 or IPv6), roaming partners, and supported authentication methods, and receive that information in Information Elements from the AP.

ArubaOS 6.4 supports several ANQP and H2QP profile types for defining Hotspot data. The following table describes the profiles in the Hotspot profile set.

Table 4: *ANQP and H2QP Profiles referenced by an Advertisement Profile*

| Profile | Description |
|--------------------------------------|---|
| Hotspot Advertisement profile | An advertisement profile defines a collection of ANQP and H2QP profiles. Each hotspot 2.0 profile is associated with one advertisement profile, which in turn references one of each type of ANQP and H2QP profile. |
| ANQP 3GPP Cellular Network profile | Use this profile to define priority information for a 3rd Generation Partnership Project (3GPP) Cellular Network used by hotspots that have roaming relationships with cellular operators. |
| ANQP Domain Name profile | Use this profile to specify the hotspot operator domain name. |
| ANQP IP Address Availability profile | Use this profile to specify the types of IPv4 and IPv6 IP addresses available in the hotspot network. |
| ANQP NAI Realm profile | This profile identifies and describes a Network Access Identifier (NAI) realm accessible using the AP, and the method that this NAI realm uses for authentication. |
| ANQP Network Authentication profile | Use the ANQP Network Authentication profile to define the authentication type used by the hotspot network. |
| ANQP Roaming Consortium profile | Name of the ANQP Roaming Consortium profile to be associated with this WLAN advertisement profile. |

Table 4: ANQP and H2QP Profiles referenced by an Advertisement Profile

| Profile | Description |
|---|--|
| ANQP Venue Name profile | Use this profile to specify the venue group and venue type information be sent in an Access network Query Protocol (ANQP) information element in a Generic Advertisement Service (GAS) query response. |
| H2QP Connection Capability profile | Use this profile to specify hotspot protocol and port capabilities. |
| H2QP Operating Class Indication profile | Use this profile to specify the channels on which the hotspot is capable of operating. |
| H2QP Operator Friendly Name profile | Use this profile to define the operator-friendly name sent by devices using this profile. |
| H2QP WAN Metrics profile | Use this profile to specify the WAN status and link metrics for your hotspot. |

AP-220 Series Enhancements

The following enhancements have been made to the AP-220 Series access point:

- CAC and TSPEC handling
- Multi-client performance tuning

AP-130 Series Functionality Improvements when Powered Over 802.3af (POE)

Starting with ArubaOS 6.4, all features and both Ethernet ports of the AP-130 Series are supported when the AP is powered by 802.3af POE.

Franklin Wireless U770 4G Modem Support

ArubaOS 6.4 introduces support of the Franklin Wireless U770 4G USB cellular modem for the Sprint LTE service on the RAP-155.

Huawei E3276 LTE Modem Support

ArubaOS 6.4 introduces support of the Huawei E3276 LTE USB cellular modem on the RAP-3WN, RAP-108, RAP-109, and RAP-155.

Authentication

Authentication Server Limits

Starting with ArubaOS 6.4, a maximum of 128 LDAP, RADIUS, and TACACS servers, each can be configured on the controller.

EAP-MD5 Support

The controller does not support EAP-MD5 authentication for wireless clients. In ArubaOS 6.3.x and ArubaOS 6.4.x, EAP-MD5 authentication for wired clients fails. This issue is under investigation and expected to be fixed in the upcoming ArubaOS 6.3.x and ArubaOS 6.4.x patch releases.

Controller-Platform

AirGroup

Default Behavior Changes

Starting from ArubaOS 6.4, AirGroup is disabled by default. If you upgrade from an existing non-AirGroup version to AirGroup 6.4 or perform the fresh installation of ArubaOS 6.4, AirGroup is disabled by default. If you run an earlier version of ArubaOS with the AirGroup enabled and upgrade to ArubaOS 6.4, AirGroup feature is enabled.

The following AirGroup features are introduced in ArubaOS 6.4:

AirGroup DLNA UPnP Support

ArubaOS 6.4 introduces the support for DLNA (Digital Living Network Alliance), a network standard that is derived from UPnP (Universal Plug and Play) in addition to the existing mDNS protocol. DLNA uses the Simple Service Discovery Protocol (SSDP) for service discovery on the network. DLNA provides the ability to share digital media between multimedia devices like Windows and Android, similar to how mDNS supports Zero Configuration Networking to Apple® devices and services.

ArubaOS 6.4 ensures that DLNA seamlessly works with the current mDNS implementation. All the features and policies that are applicable to mDNS are extended to DLNA. This ensures full interoperability between compliant devices.

AirGroup mDNS Static Records

AirGroup processes mDNS packets advertised by servers and creates the relevant cache entries. When a query comes from a user, AirGroup responds with the appropriate cache entries with the relevant policies applied. Starting from ArubaOS 6.4, AirGroup provides the ability for an administrator to add the mDNS static records to the cache.

Group Based Device Sharing

ArubaOS 6.4 AirGroup supports the sharing of AirGroup devices such as AppleTV, or Printers to a **User Group** using CPPM. This is an enhancement to features that support device sharing based upon the user's username, user-role, and location.

AirGroup-WebUI Monitoring Dashboard Enhancements

This release of ArubaOS provides the following enhancements to the AirGroup WebUI:

- **Usage** – You can view the following enhancements in the **Usage** page of the WebUI:
 - The AirGroup service names in the **AirGroup** row are now clickable. If you click a service, you are redirected to the **Dashboard > AirGroup** page that displays a list of AirGroup servers filtered by Service Name.
- **Clients** – You can view the following enhancements in the **Clients** page of the WebUI:
 - Under **Dashboard > Clients**, a new **AirGroup** column is added to display the devices that are listed as mDNS, DLNA, or both. If a device does not support both **mDNS** and **DLNA**, this field is blank.
- **AirGroup** – You can view the following enhancements in the **AirGroup** page of the WebUI:
 - A new **AirGroup type** column is added and this column specifies if the type of the AirGroup device is mDNS, DLNA or both.
 - The MAC address of each AirGroup user and server is now clickable. If you click MAC link, you are redirected to the **Dashboard > Clients > Summary page > AirGroup** tab. If an AirGroup user or AirGroup server is a wired trusted client, the MAC address is not clickable.

AirGroup-Limitations

The AirGroup feature has the following limitations in ArubaOS 6.4:

- AirGroup's DLNA discovery works across VLANs, however, media streaming from Windows Media Server does not work across VLANs. This limitation is a result of Digital Rights Management (DRM) support in Windows Media Server, which restricts media sharing across VLANs. Media streaming works only when both client and server are connected to the same VLAN.
- Android devices cannot discover media server while using the native music and video player applications and when they are connected across VLANs. For example, Samsung Tab 3 cannot discover the media server on Samsung Galaxy S4 while using the native music and video player applications. Android devices can discover media server when they are connected in the same VLAN. This restriction is caused by Samsung devices.
- Xbox cannot be added as an extender to the Windows clients using the Windows Media Center application with the AirGroup feature enabled. You need to disable the AirGroup feature before adding Xbox as an extender.

AppRF 2.0

The AppRF 2.0 feature improves application visibility and control by allowing you to configure and view access control list (ACL), bandwidth application, and application category-specific data. AppRF 2.0 supports a Deep Packet Inspection (DPI) engine for application detection for over a thousand applications. All wired and wireless traffic that traverses the controller can now be categorized and controlled by application and application category.

AppRF 2.0 provides the ability to:

- permit or deny an application or application category for a specific role. For example, you can block bandwidth monopolizing applications on a guest role within an enterprise.
- rate limit an application or application category, such as video streaming applications, for a specific role.
- mark different L2/L3 Quality of Service (QoS) for an application or application category for a user role. For example, you can mark video and voice sessions that originate from wireless users with different priorities so that traffic is prioritized accordingly in your network.

Policy Configuration

Access control lists now contain new application and application category options that let you permit or deny an application /application category on a given role.

Global Session ACL

A new session ACL has been added named "global-sacl." This session, by default, is in position one for every user role configured on the controller. The global-sacl session ACL has the following properties:

- cannot be deleted.
- always remains at position one in every role and its position cannot be modified.
- contains only application rules.
- can be modified in the WebUI and dashboard on a master controller.
- any modifications to it results in the regeneration of ACE's of all roles.

Role Default Session ACL

You can configure role-specific application configuration using the WebUI and dashboard. For example, you can deny the facebook application on the guest role using the dashboard without having to change the firewall configuration.

A new role session ACL named `apprf-"role-name"-sac1` has been added. This session, by default, is in position one for every user role configured on the controller.

The string "apprf" is added to the beginning and "sac1" to the end of a role's name to form a unique name for role default session ACL. This session ACL is in position 2 of the given user role after the global session ACL and takes the next higher priority after global policy rules.

The predefined role session ACL has the following properties:

- cannot be deleted through the WebUI or CLI. It is only deleted automatically when the corresponding role is deleted.
- always remains at position 2 in every role and its position cannot be modified.
- contains only application rules.
- can be modified using the WebUI or dashboard on a master controller, however any modification results in the regeneration of ACE's for that role.
- cannot be applied to any other role.

Bandwidth Contract Configuration

Bandwidth contract configuration lets you configure bandwidth contracts for both the global or application-specific levels.

Global Bandwidth Contract Configuration

You can configure bandwidth contracts to limit application and application categories on an application or global level.

Role-Specific Bandwidth Contracts

Application-specific bandwidth contracts (unlike "generic" bandwidth-contracts) allow you to control or reserve rates for specific applications only on a per-role basis. An optional exclude list is provided that allows you to exclude applications or application categories on which a generic user/role bandwidth-contract is not applied. The exclude list enables you to give specific enterprise applications priority over other user traffic.

Important points regarding bandwidth contracts include:

- Application bandwidth contracts are per-role by default.
- When an application bandwidth-contract is configured for both a category and an application within the category, always apply the most specific bandwidth contract.

AppRF Dashboard Application Visibility

The AppRF Dashboard Application Visibility feature allows you to configure both application and application category policies within a given user role.

The **AppRF** page on the **Dashboard** tab displays the PEF summary of all the sessions in the controller aggregated by users, devices, destinations, applications, WLANs, and roles. The elements are now represented in box charts instead of pie charts.



Applications and Application Categories containers are only displayed on 7200 Series controllers. The remaining controller platforms will retain ArubaOS 6.3.x.x Firewall charts (i.e. without new application classification box chart).

Branch

Centralized BID Allocation

In Master-Local controller set-up, the Master controller runs the BID allocation algorithm and allocates BID to the branches terminating on it and to the Local controllers. The Master controller saves the BIDs in its memory IAP database to avoid the collision of BID (per subnet) whereas the Local controller saves the BIDs only in its in

memory data structures. The IAP manager in Local controller forwards only the new register request (branch coming for the first time with BIDs as -1) message to the Master controller. For existing branch's register request, the Local controller tries to honor the requested BIDs first. The master and local communication is within the existing IPsec tunnel. The Master controller gets the register request and allocates BIDs using the BID allocation algorithm. Finally, the Master controller sends back the allocated BIDs to the Local controller and the Local controller updates its data structure and sends the response to the IAP.

General guidelines for upgrading from existing IAP-VPN release to ArubaOS 6.4:

1. Ensure that all the branches are upgraded to Instant 4.0.
2. Upgrade the data-center to ArubaOS 6.4.



If you have a Master-Local setup; upgrade the Master controller first and then the Local controller.

3. Ensure that always the IAP-VPN branches are configured using authorized tools like AirWave/Athena, else you must trust all branches or the required branch using the following command,

```
iap trusted-branch-db allow-all
```

or

```
iap trusted-branch-db add mac-address<mac-address>
```



Instant version earlier than 4.0 also need the previous command to be executed for the controller to come up with ArubaOS 6.4.

Controller LLDP Support

ArubaOS 6.4 provides support for Link Layer Discovery Protocol (LLDP) on controllers to advertise identity information and capabilities to other nodes on the network, and store the information discovered about the neighbors.

High Availability

This section describes High Availability features added or modified in ArubaOS 6.4.

High Availability Configuration Using the WebUI

The high availability profiles introduced in ArubaOS 6.3 can now be configured using the **Configuration > Advanced Services Redundancy** window of the ArubaOS 6.4 WebUI. In previous releases, high availability profiles were configured in the **HA** section of the **Configuration > Advanced Services > All Profile Management** window. This section of the WebUI is removed in ArubaOS 6.4.

Client State Synchronization

State synchronization improves failover performance by synchronizing client authentication state information from the active controller to the standby controller, allowing clients to authenticate on the standby controller without repeating the complete 802.1X authentication process. This feature requires you to configure the high availability group profile with a pre-shared key. The controllers use this key to establish the IPsec tunnels through which they send state synchronization information.

The state synchronization feature limits each high availability group to one IPv4 standby controller and one IPv6 standby controller, or one pair of dual-mode IPv4 and IPv6 controllers. Therefore, this feature can only be enabled in high-availability deployments that use the following topologies for each IPv4 or IPv6 controller pair.

- **Active/Active Model:** In this model, two controllers are deployed in dual mode. Controller one acts as a standby for the APs served by controller two, and vice-versa. Each controller in this deployment model supports approximately 50% of its total AP capacity, so if one controller fails, all the APs served by that

controller will fail over to the other controller, thereby providing high availability redundancy to all APs in the cluster.

- **Active/Standby Model:** In this model, the active controller supports up to 100% of its rated capacity of APs, while the other controller in standby mode is idle. If the active controller fails, all APs served by the active controller will failover to the standby controller.

High Availability Inter-controller Heartbeats

The high availability inter-controller heartbeat feature allows faster AP failover from an active controller to a standby controller, especially in situations where the active controller reboots or loses connectivity to the network.

The inter-controller heartbeat feature works independently from the AP mechanism that sends heartbeats from the AP to the controller. If enabled, the inter-controller heartbeat feature supersedes the AP's heartbeat to its controller. As a result, if a standby controller detects missed inter-controller heartbeats from the active controller, it triggers the standby APs to failover to the standby controller, even if those APs have not detected any missed heartbeats between the APs and the APs' active controller.



Use this feature with caution in deployments where the active and standby controllers are separated over high-latency WAN links.

When this feature is enabled, the standby controller starts sending regular heartbeats to an AP's active controller as soon as the AP has an UP status on the standby controller. The standby controller initially flags the active controller as *unreachable*, but changes its status to *reachable* as soon as the active controller sends a heartbeat response. If the active controller later becomes unreachable for the number of heartbeats defined by the heartbeat threshold (by default, five missed heartbeats), the standby controller immediately detects this error, and informs the APs using the standby controller to fail over from the active controller to the standby controller. If, however, the standby controller never receives an initial heartbeat response from the active controller, and therefore never marks the active controller as initially reachable, the standby controller will not initiate a failover.

Extended Standby Controller Capacity

The standby controller over-subscription feature allows a standby controller to support connections to standby APs beyond the controller's original rated AP capacity. This feature is an enhancement from the high availability feature introduced in ArubaOS 6.3, which requires the standby controller have a AP capacity equal to or greater than the total AP capacity of all the active controllers it supports.

Starting with ArubaOS 6.4, a 7200 Series controller acting as a standby controller can oversubscribe to standby APs by up to four times that controller's rated AP capacity, and a standby M3 controller module or 3600 controller can oversubscribe by up to two times its rated AP capacity, as long as the tunnels consuming the standby APs do not exceed the maximum tunnel capacity for that standby controller.



3200XM, 3400, and 600 Series controllers do not support this feature.

Features not Supported on 600 Series Controllers

The 600 Series controller platforms do not support the following features in ArubaOS 6.4.

- AirGroup
- AppRF 1.0/Firewall Visibility
- IF-MAP
- AP Image Preload
- Centralized Image Upgrade

- IAP-VPN

Control Plane Bandwidth Contracts Values

Beginning with ArubaOS 6.4, control plane bandwidth contracts are configured in packets per second (pps) instead of bits per second (bps). This makes performance more predictable. The bandwidth contract range is now 1 to 65536 pps. Additionally, show commands related to control plane bandwidth contracts display pps. The formula used to convert bps to pps is **pps=bps/(256 x 8)**.

Automatic GRE from IAP

ArubaOS 6.4 introduces automatic GRE tunnel formation between the controller and Instant access points. Manual configuration of GRE is no longer required on the controller. This feature uses the existing IPSec connection with the controller to send control information to set up the GRE tunnel. Since the GRE control information is exchanged through a secure tunnel, security and authentication is addressed.

DHCP Lease Limit

The following table provides the maximum number of DHCP leases supported per controller platform.

Table 5: *DHCP Lease Limit*

| Platform | DHCP Lease Limit |
|----------|------------------|
| 620 | 256 |
| 650/651 | 512 |
| 3200XM | 512 |
| 3400 | 512 |
| 3600, M3 | 512 |
| 7210 | 5120 |
| 7220 | 10240 |
| 7240 | 15360 |

IPv6

This section describes IPv6 features added or modified in ArubaOS 6.4.

Multicast Listener Discovery (MLDv2) Snooping

This release of ArubaOS supports Source Specific Multicast (SSM) and Dynamic Multicast Optimization (DMO) as part of the IPv6 MLDv2 feature.

Source Specific Multicast

The Source Specific Multicast (SSM) supports delivery of multicast packets that originate only from a specific source address requested by the receiver. You can forward multicast streams to the clients if the source and group match the client subscribed source group pairs (S,G).

The controller supports the following IPv6 multicast source filtering modes:

- Include - In Include mode, the reception of packets sent to a specified multicast address is enabled only from the source addresses listed in the source list. The default IPv6 SSM address range is FF3X::4000:1 – FF3X::FFFF:FFFF, and the hosts subscribing to SSM groups can only be in the Include mode.

- Exclude - In Exclude mode, the reception of packets sent to a specific multicast address is enabled from all source addresses. If there is a client in the Exclude mode, the subscription is treated as an MLDv1 join.

Dynamic Multicast Optimization

In a scenario where multiple clients are associated to an AP and one client subscribes to a multicast stream, all clients associated to the AP receive the stream, as the packets are directed to the multicast MAC address. To restrict the multicast stream to only subscribed clients, Dynamic Multicast Optimization (DMO) sends the stream to the unicast MAC address of the subscribed clients. DMO is currently supported for both IPv4 and IPv6.

Understanding MLDv2 Limitations

The following are the MLDv2 limitations:

- Controller cannot route multicast packets.
- For mobility clients mld proxy should be used.
- VLAN pool scenario stream is forwarded to clients in both the VLANs even if the client from one of the VLANs is subscribed.
- DMO is not applicable for wired clients in controllers.

Static IPv6 GRE Tunnel Support

Static IPv6 L2/L3 GRE tunnels can be established between Aruba devices and other devices that support IPv6 GRE tunnel. IPv4 and IPv6 L2 GRE tunnels carry both IPv6 and IPv4 traffic. The IPv6 traffic can also be redirected over the IPv4 L3 GRE tunnel.

The following options for directing traffic into the tunnel are introduced for IPv6:

- Static route, redirects traffic to the IP address of the tunnel.
- Firewall policy (session-based ACL), redirects traffic to the specified tunnel ID.



If a VLAN interface has multiple IPv6 addresses configured, one of them is used as the tunnel source IPv6 address. If the selected IPv6 address is deleted from the VLAN interface, then the tunnel source IP is re-configured with the next available IPv6 address.

Important Points to Remember

- By default a GRE Tunnel Interface is in IPv4 L3 mode.
- IPv6 configurations are allowed on an IPv4 Tunnel only if the tunnel mode is set to IPv6. Similarly, IPv4 configurations are allowed on an IPv6 Tunnel only if the tunnel mode is set to IP.

Understanding Static IPv6 GRE Tunnel Limitations

ArubaOS does not support the following functions for Static IPv6 GRE Tunnels:

- IPv6 Auto configuration and IPv6 Neighbor Discovery mechanisms do not apply to IPv6 tunnels.
- Tunnel encapsulation limit and MTU discovery options on the IPv6 tunnels.
- You cannot use IPv6 GRE for a master-local setup as IPSec is not supported in this release.

IGMPv3 Support

ArubaOS 6.4 supports IGMPv3 functionality that makes Aruba controller aware of Source Specific Multicast (SSM) and optimizes network bandwidth. The SSM functionality is an extension of IP multicast where the datagram traffic is forwarded to receivers from only those multicast sources to which the receivers have explicitly joined. By default, the multicast group range of 232.0.0.0 through 232.255.255.255 (232/8) is reserved for SSM by IANA (Internet Assigned Numbers Authority).

IPv6 Enhancements

This release of ArubaOS provides the following IPv6 enhancements on the AP:

- DNS based ipv6 controller discovery
- FTP support for image upgrade in an IPv6 network
- DHCPv6 client support

VRRPv3 Support on Controllers

Virtual Router Redundancy Protocol (VRRP) eliminates a single point of failure by providing an election mechanism, among the controllers, to elect a master controller. The master controller owns the configured virtual IPv6 address for the VRRP instance. When the master controller becomes unavailable, a backup controller steps in as the master and takes ownership of the virtual IPv6 address.

VRRPv2 support over IPv4 is already present on the Aruba Mobility Controllers. VRRPv3 support over IPv6 is introduced in the current version of ArubaOS.

Depending on your redundancy solution, you can configure the VRRP parameters on your master and local controllers. The following parameters are added in this release.

- IP version - Select IPv4 \ IPv6 from the drop-down list.
- IP \ IPv6 Address - Based on the selection made in the IP version field, either IP Address \ IPv6 Address is displayed. This is the virtual IP address that is owned by the elected VRRP master. Ensure that the same IP address and VRRP ID is used on each member of the redundant pair. Note: The IP address must be unique and cannot be the loopback address of the controller. Only one global IPv6 address can be configured on a VRRP instance.

Understanding VRRP Limitations

- It is not recommended to enable preemption on the master redundancy model. If preemption is disabled and if there is a failover, the new primary controller remains the primary controller even when the original master is active again. The new primary controller does not revert to its original state unless forced by the administrator. Disabling preemption prevents the master from “flapping” between two controllers and allows the administrator to investigate the cause of the outage.
- VRRP v2 over IPv4 supports the master-master redundancy model. However, this support is not available in VRRP v3 over IPv6. This model will be supported once support for IPsec over IPv6 is added. Currently only master-local and local-local redundancy are supported.

Security

Palo Alto Networks Firewall Integration

User-Identification (User-ID) feature of the Palo Alto Networks (PAN) firewall allows network administrators to configure and enforce firewall policies based on user and user groups. User-ID identifies the user on the network based on the IP address of the device which the user is logged into. Additionally, firewall policy can be applied based on the type of device the user is using to connect to the network. Since the Aruba controller maintains the network and user information of the clients on the network, it is the best source to provide the information for the User-ID feature on the PAN firewall.

Application Single Sign-On Using L2 Network Information

This feature allows single sign-on (SSO) for different web-based applications using Layer 2 authentication information. Single sign-on for web-based application uses Security Assertion Markup Language (SAML), which happens between the web service provider and an identity provider (IDP) that the web server trusts. A request made from the client to a web server is redirected to the IDP for authentication. If the user has already been authenticated using L2 credentials, the IDP server already knows the authentication details and returns a SAML

response, redirecting the client browser to the web-based application. The user enters the web-based application without needing to enter the credentials again.

Enabling application SSO using L2 network information requires configuration on the controller and on the IDP server. The Aruba ClearPass Policy Manager (CPPM) is the only IDP supported.

802.11w Support

ArubaOS supports the IEEE 802.11w standard, also known as Management Frame Protection (MFP). MFP makes it difficult for an attacker to deny service by spoofing Deauth and Disassoc management frames.

MFP is configured on a virtual AP (VAP) as part of the **wlan ssid-profile**. There are two parameters that can be configured; **mfp-capable** and **mfp-required**. Both the parameters are disabled by default.

Ability to Disable Factory-Default IKE/IPsec Profiles

This feature enables you to disable default IKE policies, default IPsec dynamic maps, and site-to-site IPsec maps. You can do this by using the **crypto isakmp policy**, **crypto dynamic-map**, and **crypto-local ipsec-map** CLI commands. Or, use the WebUI and navigate to **Advanced Services > VPN Services > IPSEC** and **Advanced Services > VPN Services > Site-To-Site**.

AOS/ClearPass Guest Login URL Hash

This feature enhances the security for the ClearPass Guest login URL. A new parameter called **url_hash_key** (disabled by default) has been added to the Captive Portal profile so that ClearPass can trust and ensure that the client MAC address in the redirect URL has not been tampered by anyone.

Authentication Server Load Balancing

Load balancing of authentication servers ensures that the authentication load is split across multiple authentication servers, thus avoiding any one particular authentication server from being overloaded. Authentication Server Load Balancing functionality enables the Aruba Mobility Controller to perform load balancing of authentication requests destined to external authentication servers (Radius/LDAP etc). This prevents any one authentication server from having to handle the full load during heavy authentication periods, such as at the start of the business day.

Enhancements in the User Authentication Failure Traps

The output of the **show snmp trap-queue** command has been enhanced to support the information such as Server IP address, user MAC, AP name, authentication failure details, authentication request time out, authentication server down, and up traps messages that are sent to the host.

RADIUS Accounting on Multiple Servers

ArubaOS 6.4 provides support for the controllers to send RADIUS accounting to multiple RADIUS servers. The controller notifies all the RADIUS servers to track the status of authenticated users. Accounting messages are sent to all the servers configured in the server group in a sequential order.

RADIUS Accounting for VIA and VPN Users

RADIUS Accounting is now supported for VIA and VPN users. A knob has been added under the **AAA Authentication VIA Auth profile** and the **AAA Authentication VPN profile** to enable this feature.

Spectrum Analysis

AP Platform Support for Spectrum Analysis

Starting with ArubaOS 6.3.1.0 and ArubaOS 6.4, AP-120 Series access points do not support the spectrum analysis feature, and cannot be configured as a spectrum monitor or hybrid AP.

Voice and Video

Unified Communication and Collaboration

This section describes the Unified Communication and Collaboration (UCC) feature introduced in ArubaOS 6.4. The Unified Communications Manager (UCM) is the core solution component of this feature. UCC addresses the onslaught of mobile devices that use voice, video, and collaboration applications. This reduces the cost of voice infrastructure for communication and collaboration needs.

UCC continues to support all existing functionality provided by ArubaOS 6.3.x. Following are the new sub-features introduced in ArubaOS 6.4.

- UCC Dashboard in the WebUI
- UCC **show** commands
- UCC— AirWave Integration
- Changes to Call Admission Control
- Per User Role Lync Call Prioritization
- Dynamically Open Firewall for UCC Clients using STUN
- UCC Call Quality Metrics

AP Support

ArubaOS 6.3.x.x will be the last release to support the RAP-5 access point. ArubaOS 6.3 will be supported at least through October 31st 2018. Individual AP support dates will vary based on their end of sale date. See the Aruba end of support page

<http://www.arubanetworks.com/support-services/end-of-life-products/> for additional details.

Table 6: *AP Support*

| AP Model | End of Sale Dates (Standard Variants) | Last ArubaOS Version Supported |
|--|---------------------------------------|--------------------------------|
| AP-60, AP-61, AP-65, AP-65WB, AP-70 (All Variants) | 31-May-2011 | ArubaOS 6.3 |
| AP-85 (All Variants) | 30-Apr-2013 | ArubaOS 6.3 |
| AP-120, AP-121 (802.11a/b/g) | 31-Jan-2012 | ArubaOS 6.4 |
| AP-120, AP-121 (802.11a/n or 802.11b/g/n) | 31-Jan-2012 | ArubaOS 6.4 |
| AP-124, AP-125 (802.11a/b/g) | 1-Aug-2013 | ArubaOS 6.4 |
| AP-124, AP-125 (802.11a/n and 802.11b/g/n) | 1-Aug-2013 | ArubaOS 6.4 |
| RAP-2WG | 31-Oct-2013 | ArubaOS 6.3 |
| RAP-5WN | 31-Oct-2013 | ArubaOS 6.3 |
| RAP-5 | 31-Jan-2012 | ArubaOS 6.3 |

MIB and Trap Enhancements

Modified Traps

The following traps are modified in ArubaOS 6.4:

- wlsxMgmtUserAuthenticationFailed
- wlsxNUserAuthenticationFailed
- wlsxNAuthServerReqTimeOut
- wlsxNAuthServerTimeOut
- wlsNAuthServerIsDown
- wlsNAuthServerUp

This chapter describes the regulatory updates in ArubaOS 6.4.x release versions.



Contact your local Aruba sales representative on device availability and support for the countries listed in the following tables.

Periodic regulatory changes may require modifications to the list of channels supported by an AP. For a complete list of channels supported by an AP using a specific country domain, access the controller command-line interface and issue the command **show ap allowed-channels country-code <country-code> ap-type <ap-model>**.

Regulatory Updates in ArubaOS 6.4.2.1

Table 7: *Regulatory Domain Updates*

| Regulatory Domain | Regulatory Changes |
|-------------------|--|
| Argentina | Support added for AP-274 and AP-275 |
| Australia | Support added for AP-103H |
| Bolivia | Support added for AP-225 |
| Botswana | Support added for AP-225 |
| Brazil | Support added for AP-103 |
| Canada | DFS channels added for AP-204 and AP-205 |
| Chile | <ul style="list-style-type: none"> Support added for AP-103H Support added for AP-214 and AP-215 |
| China | Support added for AP-214 and AP-215 |
| Hong Kong | <ul style="list-style-type: none"> Support added for AP-103H Support added for AP-214 and AP-215 |
| India | <ul style="list-style-type: none"> Support added for AP-204 and AP-205 Support added for AP-214 and AP-215 |
| Japan | Support added for AP-103H |
| Malaysia | Support added for AP-204 and AP-205 |
| Mauritius | Support added for AP-135 |
| Morocco | Support added for AP-225 |
| Mexico | Support added for AP-204 and AP-205 |

Table 7: *Regulatory Domain Updates*

| Regulatory Domain | Regulatory Changes |
|----------------------|--|
| New Zealand | Support added for AP-103H |
| Philippines | Support added for AP-103H |
| Quatar | Support added for AP-214 and AP-215 |
| Saudi Arabia | Support added for AP-103H |
| Singapore | <ul style="list-style-type: none"> Support added for AP-214 and AP-215 Support added for AP-103H |
| South Africa | <ul style="list-style-type: none"> Support added for AP-103H Support added for AP-204 and AP-205 |
| South Korea | <ul style="list-style-type: none"> Support added for AP-204 and AP-205 Support added for AP-274 and AP-275 |
| Taiwan | <ul style="list-style-type: none"> Support added for AP-103 Support added for AP-204 and AP-205 |
| United Arab Emirates | Support added for AP-103H |
| Ukraine | Support added for AP-103H |
| Venezuela | Channels 36-48 for 802.11a 80MHz (outdoor) |

Regulatory Updates in ArubaOS 6.4.2.0

Table 8: *Regulatory Domain Updates*

| Regulatory Domain | Change |
|--------------------|---|
| Argentina | <ul style="list-style-type: none"> Support added for AP-103 |
| Australia | <ul style="list-style-type: none"> Support added for AP-204 and AP-205 |
| Austria | <ul style="list-style-type: none"> Support added for AP-103H Support added for AP-214 and AP-215 |
| Bahamas | <ul style="list-style-type: none"> Support added for AP-204 and AP-205 Support added for AP-224 and AP-225 Support added for AP-274 and AP-275 |
| Bosnia/Herzegovina | <ul style="list-style-type: none"> Support added for AP-103H |
| Belgium | <ul style="list-style-type: none"> Support added for AP-103H Support added for AP-214 and AP-215 |
| Bulgaria | <ul style="list-style-type: none"> Support added for AP-103H Support added for AP-214 and AP-215 |

| Regulatory Domain | Change |
|--------------------|--|
| Canada | <ul style="list-style-type: none"> Support added for AP-103H Support added for AP-214 and AP-215 |
| China | <ul style="list-style-type: none"> Support added for AP-275 |
| Chile | <ul style="list-style-type: none"> Support added for AP-274 and AP-275 |
| Colombia | <ul style="list-style-type: none"> FCC DFS channels added to AP-224 and AP-225 Support added for AP-103H |
| Croatia | <ul style="list-style-type: none"> Support added for AP-103H Support added for AP-214 and AP-215 |
| Cyprus | <ul style="list-style-type: none"> Support added for AP-103H |
| Czech Republic | <ul style="list-style-type: none"> Support added for AP-103H Support added for AP-214 and AP-215 |
| Denmark | <ul style="list-style-type: none"> Support added for AP-103H Support added for AP-214 and AP-215 |
| Dominican Republic | <ul style="list-style-type: none"> FCC DFS channels added to AP-224 and AP-225 |
| Estonia | <ul style="list-style-type: none"> Support added for AP-103H Support added for AP-214 and AP-215 |
| Finland | <ul style="list-style-type: none"> Support added for AP-103H Support added for AP-214 and AP-215 |
| France | <ul style="list-style-type: none"> Support added for AP-103H Support added for AP-214 and AP-215 |
| Germany | <ul style="list-style-type: none"> Support added for AP-103H Support added for AP-214 and AP-215 |
| Hong Kong | <ul style="list-style-type: none"> Support added for AP-204 Channels 141-165 enabled for AP-120, AP-121, AP-124, and AP-125 Support added for AP-224 and AP-225 |
| Hungary | <ul style="list-style-type: none"> Support added for AP-103H Support added for AP-214 and AP-215 |
| India | <ul style="list-style-type: none"> Support added for AP-274 and AP-275 |
| Ireland | <ul style="list-style-type: none"> Support added for AP-103H Support added for AP-214 and AP-215 |
| Israel | <ul style="list-style-type: none"> Support ended for 802.11g 40MHz (indoor) 8-12 and 9-13 Support ended for 802.11g 40MHz (outdoor) 8-12 and 9-13 |
| Italy | <ul style="list-style-type: none"> Support added for AP-103H Support added for AP-214 and AP-215 |
| Japan | <ul style="list-style-type: none"> Support added for AP-204 and AP-205 |

| Regulatory Domain | Change |
|-------------------|--|
| Israel | <ul style="list-style-type: none"> Support added for AP-204 and AP-205 |
| Latvia | <ul style="list-style-type: none"> Support added for AP-103H Support added for AP-214 and AP-215 |
| Lithuania | <ul style="list-style-type: none"> Support added for AP-103H Support added for AP-214 and AP-215 |
| Luxembourg | <ul style="list-style-type: none"> Support added for AP-103H Support added for AP-214 and AP-215 |
| Macedonia | <ul style="list-style-type: none"> Support added for AP-204 and AP-205 Support added for AP-103H |
| Malta | <ul style="list-style-type: none"> Support added for AP-103H Support added for AP-214 and AP-215 |
| Maritime | <ul style="list-style-type: none"> Support added for AP-68 Support added for AP-92, AP-93, and AP-93H Support added for AP-103H, AP-104, and AP-105 Support added for AP-120, AP-121, AP-124, and AP-125 Support added for AP-134 and AP-135 Support added for AP-175DC, AP-175AC, and AP-175P Support added for AP-204 and AP-205 Support added for AP-224 and AP-225 Support added for RAP-3WN and RAP-3WNP |
| Maritime Offshore | <ul style="list-style-type: none"> Support added for AP-68 Support added for AP-92, AP-93, and AP-93H Support added for AP-103H, AP-104, and AP-105 Support added for AP-120, AP-121, AP-124, and AP-125 Support added for AP-134 and AP-135 Support added for AP-175DC, AP-175AC, AP-175P Support added for AP-204 and AP-205 Support added for AP-224 and AP-225 Support added for RAP-3WN and RAP-3WNP |
| Mauritius | <ul style="list-style-type: none"> Support added for AP-224 and AP-225 |
| Mexico | <ul style="list-style-type: none"> Support added for AP-103 |
| Montenegro | <ul style="list-style-type: none"> Support added for AP-103H |
| Netherlands | <ul style="list-style-type: none"> Support added for AP-103H Support added for AP-214 and AP-215 |
| New Zealand | <ul style="list-style-type: none"> Support added for AP-204 and AP-205 |
| Philippines | <ul style="list-style-type: none"> Support added for RAP-108 Support added for AP-204 and AP-205 |
| Poland | <ul style="list-style-type: none"> Support added for AP-103H Support added for AP-214 and AP-215 |

| Regulatory Domain | Change |
|--------------------------|---|
| Portugal | <ul style="list-style-type: none"> Support added for AP-103H Support added for AP-214 and AP-215 |
| Puerto Rico | <ul style="list-style-type: none"> FCC DFS channels added to AP-224 and AP-225 Support added for AP-103H Support added for AP-274 and AP-275 |
| Qatar | <ul style="list-style-type: none"> Support added for AP-204 and AP-205 |
| Romania | <ul style="list-style-type: none"> Support added for AP-103H Support added for AP-214 and AP-215 |
| Saudi Arabia | <ul style="list-style-type: none"> Support added for AP-204 and AP-205 |
| Slovakia | <ul style="list-style-type: none"> Support added for AP-103H Support added for AP-214 and AP-215 |
| Slovenia | <ul style="list-style-type: none"> Support added for AP-103H Support added for AP-214 and AP-215 |
| South Africa | <ul style="list-style-type: none"> Support added for AP-274 and AP-275 |
| South Korea | <ul style="list-style-type: none"> Support added for AP-274 and AP-275 |
| Sweden | <ul style="list-style-type: none"> Support added for AP-103H |
| Thailand | <ul style="list-style-type: none"> Support added for AP-103H |
| Ukraine | <ul style="list-style-type: none"> Support added for AP-204 and AP-205 |
| United Kingdom | <ul style="list-style-type: none"> Support added for AP-103H Support added for AP-214 and AP-215 |
| United States of America | <ul style="list-style-type: none"> Support added for AP-103H Support added for AP-214 and AP-215 |
| Venezuela | <ul style="list-style-type: none"> Support added for AP-225 |
| Vietnam | <ul style="list-style-type: none"> Support added for AP-225 Support added for AP-115 |

Regulatory Updates in ArubaOS 6.4.0.2

The following table describes regulatory enhancements introduced in ArubaOS 6.4.0.2.

Table 9: *Regulatory Domain Updates*

| Regulatory Domain | Change |
|-------------------|---|
| India | <ul style="list-style-type: none"> Support for AP-175DC access point |
| Senegal | <ul style="list-style-type: none"> Support for AP-134 and AP-135 access points |

Regulatory Updates in ArubaOS 6.4.0.0

The following table describes regulatory enhancements introduced in ArubaOS 6.4.0.0.

Table 10: *Regulatory Domain Updates*

| Regulatory Domain | Change |
|---|--|
| Argentina, Uruguay, and Vietnam | <ul style="list-style-type: none">Support for AP-92 and AP-93 access points |
| Uruguay | <ul style="list-style-type: none">Support for AP-104 and AP-105 access points |
| Argentina, Chile, Israel, and Taiwan | <ul style="list-style-type: none">Support for RAP-108 and RAP-109 access points |
| Thailand, Indonesia | <ul style="list-style-type: none">Support for the RAP-109 remote access point |
| Australia, Argentina, Brazil, Chile, China, Colombia, Egypt, Hong Kong, India, Indonesia, Israel, Malaysia, Mexico, New Zealand, Qatar, Russia, Saudi Arabia, Singapore, South Korea, South Africa, Taiwan, Thailand, Trinidad and Tobago, UAE, and Ukraine | <ul style="list-style-type: none">Support for AP-114 and AP-115 access points |
| Australia, Chile, China, Egypt, Hong Kong, India, Indonesia, Israel, Japan, Malaysia, Mexico, New Zealand, Qatar, Russia, Saudi Arabia, Singapore, South Africa, Taiwan, Thailand, and Ukraine | <ul style="list-style-type: none">Support for RAP-155 and RAP-155P access points |
| Costa Rica | <ul style="list-style-type: none">Support for AP-134 and AP-135 access points |
| Indonesia | <ul style="list-style-type: none">Support for AP-175 access points |
| Nigeria | <ul style="list-style-type: none">Support for AP-105 access points |
| Argentina, Brazil, Chile, India, Indonesia, Israel, Mexico, Philippines, Russia, Taiwan, Trinidad and Tobago, and Ukraine | <ul style="list-style-type: none">Support for AP-224 and AP-225 access points |

| Regulatory Domain | Change |
|------------------------------|---|
| China | <ul style="list-style-type: none"> Support for the AP-224 access point |
| Argentina, Chile, and Israel | <ul style="list-style-type: none"> Support for the RAP-3WN and RAP-3WNP access points |
| Serbia and Montenegro | <ul style="list-style-type: none"> In addition to the CS country code used for both Serbia and Montenegro combined, ArubaOS now supports the RS country code for Serbia and the ME country code for Montenegro. |

The following example shows indoor, outdoor and DFS channels supported by an AP-105 in the **United States** domain.

```
(host) #show ap allowed-channels country-code us ap-type 105
Allowed Channels for AP Type 105 Country Code "US" Country "United States"
-----
PHY Type                Allowed Channels
-----
802.11g (indoor)         1 2 3 4 5 6 7 8 9 10 11
802.11a (indoor)         36 40 44 48 52 56 60 64 100 104 108 112 116 132 136 140 149 153 157
161 165
802.11g (outdoor)        1 2 3 4 5 6 7 8 9 10 11
802.11a (outdoor)        52 56 60 64 100 104 108 112 116 132 136 140 149 153 157 161 165
802.11g 40MHz (indoor)    1-5 2-6 3-7 4-8 5-9 6-10 7-11
802.11a 40MHz (indoor)    36-40 44-48 52-56 60-64 100-104 108-112 132-136 149-153 157-161
802.11g 40MHz (outdoor)   1-5 2-6 3-7 4-8 5-9 6-10 7-11
802.11a 40MHz (outdoor)   52-56 60-64 100-104 108-112 132-136 149-153 157-161
802.11a (DFS)            52 56 60 64 100 104 108 112 116 132 136 140
```


This chapter describes the issues resolved in ArubaOS 6.4.x release versions.

Resolved Issues in ArubaOS 6.4.2.1

The following issues are resolved in ArubaOS 6.4.2.1.

Activate

Table 11: *Activate Fixed Issues*

| Bug ID | Description |
|--------|--|
| 105345 | <p>Symptom: When the active whitelist feature was enabled and the controller downloaded the whitelist from the Active Server, the customer's account credentials were logged in the active logs. These logs were enabled only when the logging level was set to debugging. The fix ensures that the logs that are retrieving the activate HTTP message content is removed.</p> <p>Scenario: This issue was observed in controllers running ArubaOS 6.3 and later versions.</p> |

Airgroup

Table 12: *Airgroup Fixed Issues*

| Bug ID | Description |
|--------|--|
| 102648 | <p>Symptom: mDNS process crashed frequently. This issue is resolved by making code level changes to obtain the switch MAC address in a robust manner.</p> <p>Scenario: This issue was observed in 7200 Series controllers running ArubaOS 6.4.0.3.</p> |

Air Management-IDS

Table 13: *Air Management-IDS Fixed Issues*

| Bug ID | Description |
|--------|---|
| 106242 | <p>Symptom: The initial RSSI (Received Signal Strength Indication) value was incorrect for some wireless client entries in the AP. When creating the client entry, the AP checks if the frame was sent by the client device. If not, the controller does not update the RSSI value, and it remains unset until a frame is seen from the client device. This check resolved the issue.</p> <p>Scenario: This issue occurred only when an AP2STA (AP to station) frame was used to create the client entry. Though this frame was not initiated from the wireless client, the AP incorrectly used the RSSI from this frame to set the RSSI value for the wireless client. This issue was not limited to any specific controller model or ArubaOS release version.</p> |

AP-Platform

Table 14: *AP-Platform Fixed Issues*

| Bug ID | Description |
|--|---|
| 102260 | Symptom: Although multiple Virtual Access Points (VAPs) were enabled, only one VAP could be configured. This issue is resolved by making code level changes to the VAP configuration. Scenario: This issue was observed when multiple VAPs were enabled on a single radio. This issue was observed when the show ap debug received-config command was issued. |
| 101510 104520 104726 105296 105627 106396 106609 | Symptom: The status of an AP was displayed as UP on the local controller, but as DOWN on the master controller. The fix ensures that when there is no change in the value of the master switch IP, an update from the IKE module is rejected. Scenario: This issue was observed in M3 and 3600 controllers running ArubaOS 6.3.1.5 in a master-standby-local topology. Platform: All platforms. Reported Version: ArubaOS 6.3.1.5. Workaround: None. |
| 105417 106186 | Symptom: Although wireless clients were associated to an AP, they failed to transmit data. This issue is resolved by making code level changes to enable dos-prevention and thereby ensuring that the entities in the AP are synchronized. Scenario: This issue was observed when dos-prevention parameter in the wlan virtual-ap command was disabled. This issue was triggered when the client sent a DISASSOC frame to the AP. This issue was observed in all AP platforms running ArubaOS 6.4.1 or later versions. |
| 105529 | Symptom: When the AP restarted, the Enet1 port was used as the new active uplink. Also, the AP did not boot. This issue is fixed by ensuring that the Enet0 port is used as the primary active link. Scenario: This issue was observed in AP-224/AP-225 when the Enet1 port was connected to a laptop or a projector and the AP was using the static IP address. |

AP-Wireless

Table 15: *AP-Wireless Fixed Issues*

| Bug ID | Description |
|--|--|
| 104160 104278 104279 | Symptom: An error occurred when the hardware chip set was unable to perform self-offset calibration in 1 ms. This issue is resolved by removing unnecessary driver logs when there is a channel switch failure. Scenario: This issue occurred when the volume of error messages per day was high on the syslog server. This issue was observed in AP-115 and RAP-155 running ArubaOS 6.3.0 or later versions. |
| 104254 104922 106118 106704 106966 | Symptom: After upgrading to ArubaOS 6.4.1.0, access points de-authenticated clients with an error message Station Up Message controller Timed Out . Internal code changes ensure valid authentication of clients by access points. Scenario: Clients were unable to connect to the SSID after the controller was upgraded to ArubaOS 6.4.1.0. This issue was observed on M3 controllers running ArubaOS 6.4.1.0. |
| 105528 | Symptom: Dell laptop did not connect to AP-225 and EAP exchange failed. This issue is resolved by fixing the capability in beacon when HT is disabled. Scenario: This issue was observed in AP-225 connected to controllers running ArubaOS 6.3.1.5. |

Base OS Security

Table 16: *Base OS Security Fixed Issues*

| Bug ID | Description |
|------------------|---|
| 101355 | Symptom: The controller was not completely compliant with RFC3576 as the state attribute was not processed and sent back to the server. With this fix, the controller adheres to RFC3576. Scenario: This issue occurred when the Change of authorization (CoA) request packet sent contained a state attribute but the controller was not placing that state attribute in the CoA-Ack. This issue was not limited to a specific controller model or ArubaOS release version. |
| 102632 | Symptom: EAP-TLS termination displayed certificate verification failed error message when the controller was upgraded from ArubaOS 6.1 to ArubaOS 6.3. Changes in the certificate verification to support partial chain fixed this issue. Scenario: This issue was observed when the CA-certificate that was used for verification did not have the full chain to the Root CA. This issue was observed when the controller was configured with EAPTLS termination running ArubaOS 6.2 or later versions. |
| 103227 103355 | Symptom: The ssh mgmt-auth public-key parameter was disabled on the master controller but was not synchronized on the local controller when the value in the cfg sync-type command was set as complete . This issue is resolved by including the no ssh mgmt-auth public-key parameter in the running-config when the ssh mgmt-auth public-key parameter is disabled. Scenario: This issue occurred in a master-local setup due to the absence of a trigger on the local controller to delete ssh mgmt-auth public-key . This issue was not limited to any specific controller or ArubaOS release version. |
| 105418 | Symptom: A flaw in OpenSSL SSL/TLS server allows a man-in-the-middle attacker to force a downgrade to TLS 1.0 even if both the server and client support a higher protocol version. This issue is resolved with internal code changes. Scenario: This issue was observed in controllers running ArubaOS 6.3.x and ArubaOS 6.4.x. |
| 106066 106572 | Symptom: Authentication module crashed in 7240 controller. This issue is resolved with internal code changes. Scenario: This issue was observed in 7240 controller running ArubaOS 6.3.1.5. |

Configuration

Table 17: *Configuration Fixed Issues*

| Bug ID | Description |
|--|---|
| 95535 95582 99325 99934 104674 | Symptom: The ACL configuration on the local controller went out of sync intermittently with the master controller. The fix ensures that when centralized licensing is enabled and if PEFNG license is installed, the ACL configuration associated with the license is not be changed even if the PEFNG license is not available temporarily. Scenario: This issue occurred when there was a change in licenses. This issue was observed in controllers running ArubaOS 6.3.1.2 or later versions in a master-local topology. |
| 105688 | Symptom: The access control entries were corrupt after the controller rebooted. This issue is resolved by updating the CFGM module. Scenario: This issue was observed in a master redundancy topology after the controller was reloaded. This issue was observed in ArubaOS 6.4.0.3, but is not limited to any specific controller model. |

Controller-Datapath

Table 18: *Controller-Datapath Fixed Issues*

| Bug ID | Description |
|--------|---|
| 103223 | <p>Symptom: When netservice command with end port 65535 was executed followed by no netservice command, infinite loop of no netservice command executed. This resulted in the controller to reboot. Internal code changes ensures that the controller does not reboot after executing netservice with end port 65535 followed by no netservice command.</p> <p>Scenario: This issue was observed when netservice or no netservice commands were executed with end port value as 65535. This issue was observed in controllers running ArubaOS 6.3.x or later versions.</p> |
| 104097 | <p>Symptom: Controllers were unable to see ping requests, which resulted in ping responses being dropped. This issue is resolved by disabling the firewall enable-stateful-icmp parameter by default.</p> <p>Scenario: This issue was observed when the firewall checked for the unsolicited ICMP echo replies and dropped them if there were no ICMP echo request sessions. This issue was observed in the 7200 Series controllers and M3 controllers running ArubaOS 6.4.1.0 and above.</p> |

Controller-Platform

Table 19: *Controller-Platform Fixed Issues*

| Bug ID | Description |
|--|---|
| 95993 | <p>Symptom: Firewall visibility process crashed on a local controller. The process restarts and recovers on its own.</p> <p>Scenario: This issue was observed after a controller was running for a long duration, possibly due to overflow of an internal data structure. This issue was not limited to any specific controller model or ArubaOS release version.</p> <p>Duplicate Bugs: The following bug IDs have reported similar issues: 96671, 97943, 98502, 100384, 101190, 101795, 101852, 103097, 103689, 104252, 104638, 105502</p> |
| 103736 102443 102930 103798 103968 105499 | <p>Symptom: A controller stopped responding and rebooted. The log files for the event listed the reason as kernel module crash. This issue is resolved by enabling the watchdog petting all and watchdog respawn features.</p> <p>Scenario: This issue was observed when the watchdog process crashed. This issue was observed in 7240 controller running ArubaOS 6.4.0.2.</p> |
| 103937 | <p>Symptom: Establishing an SSH session to controller failed randomly with error message ssh_exchange_identification: Connection closed by remote host. SSH sessions were either stale or NoTTY (non-interactive session), where an SSH session did not exist but the underlying TCP connection existed. This issue is resolved by:</p> <ul style="list-style-type: none">• Performing graceful log out for all SSH sessions whose terminal was closed earlier without logging out. This clears NoTTY sessions.• Setting the parameter ClientAliveCountMax to 7200 and parameter ClientAliveInterval to 0, which terminates SSH sessions that are idle for 7200 seconds (2 hours) on the controller without killing the respective process from the shell. Disable keep alive on the SSH client so that the channel remains idle during inactivity. <p>Scenario: This issue was observed because of stale SSH processes (with NoTTY) which were unresponsive for a long duration.</p> |
| 104929 | <p>Symptom: A 7240 controller crashed when the show ap tech-support ap-name command was executed. This issue is resolved by modifying the show ap tech-support ap-name command from asynchronous mode to synchronous mode.</p> <p>Scenario: This issue was observed in APs connected to IPv4 network and in 7240 controllers running ArubaOS 6.4.0.2.</p> |

HA-Lite

Table 20: *HA-Lite Fixed Issues*

| Bug ID | Description |
|--------|--|
| 105535 | Symptom: The APs switched between active and standby controller unexpectedly due to heart beat being missed between the controllers. The issue is resolved by making internal code changes. Scenario: This issues was observed in 7240 controllers running ArubaOS 6.4.2.0. |
| 105915 | Symptom: When using fast failover, the Eth-1 wired session did not fail over. This issue is resolved by setting the cp->enable flag based on the wired-port-profile or wired-ap-profile configuration. Scenario: This issue was observed when HA failed over from active to standby in controllers running ArubaOS 6.4. |

Hotspot-11u

Table 21: *Hotspot-11u Fixed Issues*

| Bug ID | Description |
|--------|---|
| 105976 | Symptom: Although the hs2-profile was removed from the wlan virtual-ap profile, Hotspot 2.0 was not disabled completely. This issue is resolved by introducing handlers. Scenario: This issue was observed in AP-225 connected to controllers running ArubaOS 6.4.2. |

Local Database

Table 22: *Local Database Fixed Issues*

| Bug ID | Description |
|--------|--|
| 104157 | Symptom: A controller crashed due to lack of flash space. This issue is resolved by setting a size limit on log files stored in the flash memory of the controller. Scenario: This issue was observed when log files occupied most of the flash space due to multiple crashes in the database server. This issue was not limited to any specific controller model or ArubaOS release version. |

Mobility

Table 23: *Mobility Fixed Issues*

| Bug ID | Description |
|--------|--|
| 101517 | Symptom: Controller set the L3 mobility roaming state incorrectly as Home Switch/Foreign VLAN instead of Home Switch/Home VLAN when the user roamed between two SSIDs. This issue is resolved by stopping the association timer on the L3 mobility client. Scenario: This issue was observed when L3 mobility was enabled with a single WAN controller having two SSIDs, one SSID with L3 mobility enabled and the other with L3 mobility disabled. |

Station Management

Table 24: *Station Management Fixed Issues*

| Bug ID | Description |
|------------------|---|
| 102223 106169 | <p>Symptom: When the show ap association command was executed, the association table listed invalid entries. These entries were not displayed when the show user ap-name and show ap debug client-table ap-name commands were executed. The fix ensures that the send ageout parameter is called when the new node is not created and a counter is added to track the old SAP entry.</p> <p>Scenario: This issue was observed when there were a large number of mobile users. This issue was observed in AP-92, AP-105, AP-125, and AP-2255 access points connected to 7210 controller running ArubaOS 6.3.1.7.</p> |
| 102241 | <p>Symptom: The Station Management (STM) process crashed on the master controller when the ap wipe out flash command was executed. This issue is resolved by relaying the correct message to the local controller.</p> <p>Scenario: This issue was observed if an AP was present on the local controller and the ap wipe out flash command was executed on the master controller running the FIPS version of ArubaOS. This issue was observed on controllers running any version of FIPS ArubaOS.</p> |
| 104639 | <p>Symptom: Wireless clients unexpectedly failed to be in 802.11r enabled WLAN. The clients failed because the station management process crashed on the access point. Changes in the internal code of the station management module ensures clients work seamlessly in a 802.11r enabled WLAN.</p> <p>Scenario: This issue was observed when an 802.11r-capable wireless client roams from one AP to another with the same or different ESSID. In addition, this issue lasted until the client manually switched to another ESSID. This issue was observed in controllers running ArubaOS 6.3.1.8 or later versions.</p> |
| 105240 | <p>Symptom: The stm add blacklist-client command failed to add more than 512 entries whereas the previous versions of ArubaOS allowed up to 4096 entries to be added. This issue is resolved by adding a limit parameter to the client blacklist function, and allowing 4096 or 512 entries as required.</p> <p>Scenario: This issue was observed on controllers running ArubaOS 6.4.2.1.</p> |

VRRP

Table 25: *VRRP Fixed Issues*

| Bug ID | Description |
|--------|--|
| 103093 | <p>Symptom: Though Virtual Router Redundancy Protocol (VRRP) preemption was disabled on the controllers, the actual master controller did not remain as standby after it came up. The fix ensures that the actual master controller waits for the correct master rollover time calculation before assuming the role of the master controller again.</p> <p>Scenario: This issue is observed in Aruba7210 controllers when a master controller reboots and takes the role of the master controller instead of remaining in the standby role. This issue occurs due to a wrong timing calculation on Higher priority Standby.</p> |

WebUI

Table 26: *WebUI Fixed Issues*

| Bug ID | Description |
|--------|---|
| 96082 | Symptom: The Received Signal Strength Indicator (RSSI) value of a client was displayed incorrectly in the Client Monitoring page of the WebUI in Google Chrome browser. This issue is resolved by making code level changes to ensure that the correct value is displayed on all browsers. Scenario: This issue was observed when accessing the controller's WebUI using Google Chrome browser. This issue was observed in controllers running ArubaOS 6.4. |
| 100284 | Symptom: The user entered the complete MAC address when querying a whitelist-db entry. Code level changes in the search API fixed this issue and the user can now use a partial MAC address. Scenario: This issue was observed in controllers running ArubaOS 6.3.1.6. |

Resolved Issues in ArubaOS 6.4.2.0

The following issues are resolved in ArubaOS 6.4.2.0.

802.1X

Table 27: *802.1X Fixed Issues*

| Bug ID | Description |
|--------|--|
| 103635 | Symptom: When an 11r client with tunnel-mode roamed from one AP to other AP, the data traffic from the client stopped sometimes. This issue is resolved by setting a key at the controller datapath for 11r tunnel-mode stations. Scenario: This issue was observed when 11r clients, with tunnel forwarding mode enabled, roamed between APs. This issue was observed in controllers running ArubaOS 6.3.1.6. This issue was not limited to any specific controller model. |

Air Management-IDS

Table 28: *Air Management-IDS Fixed Issues*

| Bug ID | Description |
|--------|---|
| 102715 | Symptom: Ekahau/RTLS server did not parse tag frames forwarded to the server from AP-225, AP-275, or AP-205. This issue is fixed adding extra two bytes padding, in the forwarded frame, which the server expects. The padding is added by default, but it can be configured in AP system profile. Scenario: This issue was observed when using tag forwarding to Ekahau/RTLS servers from AP-225, AP-275, or AP-205 connected to controllers running ArubaOS 6.4.x. The issue does not affect Aeroscout tag forwarding. |

AP-Platform

Table 29: *AP-Platform Fixed Issues*

| Bug ID | Description |
|--------|--|
| 98995 | Symptom: AP-70 crashed when scanning an unsupported channel. This issue is resolved by changing the channel in Singapore (SG) country code and not allowing AP-70 to scan an unsupported channel. Scenario: This issue was observed in AP-70 Series devices connected to a controller running ArubaOS 6.2.1.3. |
| 103362 | Symptom: All active APs on the local controller displayed the status as down on master controller. Fixing the LMS list processing in the station management (STM) process for restart cases resolved this issue. Scenario: After an STM restart, the LMS list for the master controller was not updated in STM. This issue was observed in a master-local topology. This issue was not limited to any specific controller model and was observed in controllers running ArubaOS 6.4.1.0 or 6.3.1.8. |

AP-Wireless

Table 30: *AP-Wireless Fixed Issues*

| Bug ID | Description |
|--------|--|
| 102301 | Symptom: AP-225 rebooted unexpectedly. The log files listed the reason for the reboot as Out of Memory error . The fix ensures that the accounting error that causes AP reboot is addressed. Scenario: This issue was observed when UDP bidirectional traffic was sent using the iperf command, which resulted in an increase in traffic and RX queue. This issue was observed in AP-225 connected to controllers running ArubaOS 6.3.1.7. |
| 102631 | Symptom: When running a down-link test with best effort (BE) traffic to one client and voice traffic to another client, the voice traffic dropped to 10-12 %. This issue is fixed by setting the packet size for the UDP test to 1260 bytes or enabling MTU discovery, and not limiting the MTU to 1500 bytes. Scenario: This issue occurred when significant packets dropped before reaching the wireless driver. This issue was observed in a Server - Controller - AP - Client topology with AP-225 devices. |

ARM

Table 31: *ARM Fixed Issues*

| Bug ID | Description |
|--------|--|
| 95771 | Symptom: Scan reject did not occur when VO traffic existed. This issue is fixed by setting 802.1d priority for VO Traffic in ASAP module. Scenario: This issue was observed in AP-225 devices connected to controllers running ArubaOS 6.4.0.0. |

Authentication

Table 32: *Authentication Fixed Issues*

| Bug ID | Description |
|--------|---|
| 101664 | Symptom: On reboot, management user account which is created for Cert based GUI access gets deleted. This issue is fixed by storing the username with quotes. Scenario: This issue was observed when the management user account created for the cert based GUI access contains a space in the username. |

Base OS Security

Table 33: *Base OS Security Fixed Issues*

| Bug ID | Description |
|--------|---|
| 99882 | <p>Symptom: The down-link packets to WPA-TKIP clients randomly stopped on 7200 Series controllers. The fix ensures that issues related to support single replay counter with TKIP, which is independent of the WMM priority of the packet is addressed.</p> <p>Scenario: The issue was observed when a client used TKIP with WMM enabled. This lead to the locking of WMM queues which resulted in the client losing network connectivity.</p> |
| 101269 | <p>Symptom: The output of the show rights command displayed only partial list of session ACLs. This issue is resolved by correcting the scanning function that fetches the output in batches.</p> <p>Scenario: This issue was observed when a large number of ACLs with large number of policies were configured under a role. This issue was observed in controllers running ArubaOS 6.3.1.4 or later. This issue was not limited to any specific controller model.</p> |
| 101594 | <p>Symptom: When snmpwalk is used to query the nUser6Name Object Identifier(OID), some addresses were not retrieved. Internal code changes ensures that the subsequent IPv6 address for the same station MAC on the controller is retrieved.</p> <p>Scenario: This issue was observed when there were consecutive IPv6 addresses for the same station MAC on the controller and subsequent IPv6 address was not retrieved.</p> |
| 102480 | <p>Symptom: When a wired user moved to a new port and VLAN, the port switched to the initial role and did not repeat L2 authentication. The fix ensures that the old user entries including the ipuser entries are deleted.</p> <p>Scenario: This issue was observed when a wireless user moved from one controller to another and the DMZ controller observed the user traffic from the second GRE tunnel. L2 authentication was not initiated because the VLAN was different.</p> |

Controller-Datapath

Table 34: *Controller-Datapath Fixed Issues*

| Bug ID | Description |
|--------|--|
| 100922 | <p>Symptom: Accessing Microsoft® SharePoint using Microsoft Internet Explorer timed out. Correcting the TCP Maximum Segment Size (MSS) on the controller fixed the issue.</p> <p>Scenario: This issue was observed in controllers running ArubaOS 6.2 or later. This issue was not limited to any specific controller model.</p> |
| 101392 | <p>Symptom: In a controller, user did not appear immediately in the user-table when connected. Traffic passed through only after the user appeared in the user-table. This issue is resolved by deleting the oldest 5% of total entries during devid_cache table full condition instead of deleting only one entry so that table-full condition is not reached for consecutive new users.</p> <p>Scenario: This issue was observed in 7200 Series controllers running ArubaOS 6.3.1.3. This issue might be observed in earlier ArubaOS releases too when the devid_cache table is full and new users (who are not present in the devid-cache) come in at approximately 10 users per second. This issue was not limited to any specific controller model, but the scenario is more likely to occur on 7200 Series controllers where the maximum users are higher. Maximum devid_cache is twice the max-users and SQL sorting operations take longer along with the number of entries present.</p> |
| 103514 | <p>Symptom: After the user upgraded ArubaOS 6.4.1.0, the input error bytes on 10Gb physical interfaces were increasing. This issue is resolved by disabling 802.3 Ethernet frame length error checks on 10Gb physical interfaces.</p> <p>Scenario: This issue was observed on 7210 Series controllers running ArubaOS 6.4.0.0. This issue was observed when 802.3 Ethernet frames lengths received did match the actual number of data bytes received.</p> |

Controller-Platform

Table 35: *Controller-Platform Fixed Issues*

| Bug ID | Description |
|----------------------------|--|
| 100679 | Symptom: A 3400 controller crashed and rebooted with hardware watchdog reset. Internal code changes fixed this issue. Scenario: This issue was observed in 3200, 3400, 3600, 620, 650, and M3 controllers, but is not limited to any specific ArubaOS version. |
| 101003 | Symptom: Centralized image upgrade over TFTP did not work if the image file was in sub-directory. Centralized upgrade over TFTP worked if the image file was in root directory. Changes in the internal code fixed this issue. NOTE: The present implementation does not support absolute path. The TFTP server typically runs in sandbox. Only relative path is supported. Scenario: The download function ignored the file-path in case of download from a TFTP server. This issue was not limited to any specific controller model or ArubaOS release version. |
| 102725 103483 103558 | Symptom: The fpapps module that handles port channel management crashed and the controller rebooted. This issue is resolved by deleting a section of debug code that was not required. Scenario: This issue was caused due to the debug code added to fix bug ID 95129 and was observed on controllers running ArubaOS 6.3.1.7, 6.1.3.13, and 6.4.1.0. |
| 103715 | Symptom: The fans in the 7010 controller ran very fast and were noisy even at room temperature. This issue is resolved by fixing the fan controller algorithm to have finer granularity of RPM control vs PoE power. Scenario: This issue was observed in the controller although there was no or not much PoE load. This issue is specific to 7010 controllers running ArubaOS 6.4.1.0. |

GRE

Table 36: *GRE Fixed Issues*

| Bug ID | Description |
|--------|--|
| 103336 | Symptom: Tunnel went down due to keep-alive failure. This issue is resolved by modifying the keep-alive process to avoid packet loss. Scenario: This issue was observed when the tunnel endpoints were not in the same VLAN as the uplink VLAN through which controllers were connected. This issue was observed in controllers running ArubaOS 6.3.1.8 and was not limited to any specific controller model. |

Licensing

Table 37: *Licensing Fixed Issues*

| Bug ID | Description |
|------------------|--|
| 101443 103325 | Symptom: RAPs did not come up after upgrading from ArubaOS 6.3.1.1 (or prior) to ArubaOS 6.3.1.2 (or later). This issue is resolved by enabling the RAP feature if AP licenses exist. Scenario: This issue was observed when centralized licensing was enabled with RAPs and controllers were upgraded from ArubaOS 6.3.1.1 (or prior) to ArubaOS 6.3.1.2 (or later). The RAP feature bit was enabled in the cached bitmap on controllers running ArubaOS 6.3.1.2 which caused the upgrade issue. |

LLDP

Table 38: *LLDP Fixed Issues*

| Bug ID | Description |
|--------|--|
| 102431 | Symptom: When AP-225 was connected to a switch with a long (more than 50 m) Ethernet cable, it always worked in restricted mode even though the switch secured 19 W power by LLDP. This issue is resolved by enforcing AP-225 to work in unrestricted mode if switch can secure 19 W power by LLDP. Scenario: This issue was not limited to any specific controller model or release version. |
| 103548 | Symptom: LLDP packets were sent on boot and prior to configuration push. This issue is fixed by, not sending LLDP TLVs when AP boots, sending three mandatory TLVs (chassis subtype, port subtype and TTL) and one Aruba TLV on boot, and sending the configured TLVs after the AP receives the configuration from the controller. Scenario: This issue was observed on controllers running ArubaOS version prior to 6.4.2.0. |

QoS

Table 39: *QoS Fixed Issues*

| Bug ID | Description |
|--------|--|
| 103363 | Symptom: When the DSCP value on outer GRE IP was not set, voice quality issue was observed with Vocera badges. This issue is resolved by copying the inner DSCP value to the outer DSCP field when packet is GRE encapsulated. Scenario: This issue was observed only when WEP was enabled and not for other encryption modes. This issue was not limited to any specific controller model. |

Remote AP

Table 40: *Remote AP Fixed Issues*

| Bug ID | Description |
|--------|--|
| 99635 | Symptom: A Huawei® E160 USB modem was not functional because it lost synchronization with the RAP. This issue is resolved by making code level changes to delay the modem boot-up process for E160. Scenario: This issue was observed when the RAP connected to the USB modem was hard rebooted. |
| 101526 | Symptom: The Remote AP Authorization Profile feature was not functional when the RAP was upgraded from ArubaOS 6.2.1.0 to ArubaOS 6.3.1.6. This issue is resolved by changing the code to perform AP authorization against RAP whitelist instead of local-userdb-ap. Scenario: This issue was observed when the flag status of the RAPs did not change to Rc2 even after they were authorized by the Captive Portal user. As a result, the configuration download was incomplete. This issue was observed in ArubaOS 6.3 and above. |
| 101767 | Symptom: The Huawei® EC177 modem was not functional as it incorrectly executed script of another modem. This issue is resolved by scanning the modem twice to get the updated product ID (modem mode ID). Scenario: This issue was observed when the AP did not wait until the completion of mode-switch process for EC177. This resulted in the same product ID for both Huawei E392 and EC177. |
| 102267 | Symptom: The IAPMGR process crashed on the controller. This issue is resolved by removing the assert statement in an erroneous condition. Scenario: This issue was observed on controllers running ArubaOS 6.4 with IAPs in VPN configuration. |

Role/VLAN Derivation

Table 41: *Role/VLAN Derivation Fixed Issues*

| Bug ID | Description |
|--------|--|
| 103090 | <p>Symptom: In a network that has internal and DMZ controllers and the internal controller tunnels packets from the clients through the L2 GRE tunnel to the DMZ controller, UDR rules were not applied when a user moved as a wired user over GRE tunnel from the internal controller to the DMZ controller. This issue is resolved with internal code changes.</p> <p>Scenario: This issue was observed when using L2 GRE tunnel to send the client traffic from internal controller to DMZ controller. This issue was observed on 3600 Series controller running ArubaOS 6.3.1.8.</p> |

Station Management

Table 42: *Station Management Fixed Issues*

| Bug ID | Description |
|--------|--|
| 103452 | <p>Symptom: When a client previously associated to AP-225 left, its record showed up in show ap remote debug association table and show ap association table. This record was stale and was not removed. This issue is fixed by increasing the scb number so that the buffer reclaiming logic is not triggered often and modifying the notification to STM so that the driver does not delete a record until ageout arrives from AP STM.</p> <p>Scenario: This issue was observed in busy AP-225 where many clients were connected and the reclaiming logic was triggered. This issue was observed in AP-225 connected to controllers running ArubaOS 6.4.0.2.</p> |

WebUI

Table 43: *WebUI Fixed Issues*

| Bug ID | Description |
|--------|--|
| 103187 | <p>Symptom: User was unable to create a guest user through GPP login by using capital letters in e-mail address. This issue is resolved by allowing capital letters in e-mail address.</p> <p>Scenario: This issue was observed in controllers running ArubaOS 6.2.1.4. This issue was not limited to any specific controller model.</p> |
| 103384 | <p>Symptom: The user was unable to add port Access Control Lists (ACL) using the WebUI. This issue was fixed by making changes to the port values.</p> <p>Scenario: This issue occurred if the minimum port value was more than the maximum port value and this issue is observed on 3600 controllers running ArubaOS 6.3.1.5.</p> |

Resolved Issues in ArubaOS 6.4.1.0

The following issues are resolved in ArubaOS 6.4.1.0.

AirGroup

Table 44: *AirGroup Fixed Issues*

| Bug ID | Description |
|----------------------------|---|
| 96233 96235 96236 | <p>Symptom: An Apple® TV got dropped off from the AirGroup server list as the device got deleted from the controller cache table due to expiry of mDNS address record (A or AAAA). The fix ensures that the device is deleted from the controller cache table only if the IP address of the device matches with the expired mDNS address records (A and AAAA).</p> <p>Scenario: When an Apple TV acted as a sleep proxy server for other mDNS devices connected in the network, it advertised the address records and services of these mDNS devices. When the advertised address records of the sleeping device expired, the apple TV that acted as the sleep proxy server got deleted incorrectly. This issue is not limited to any specific controller model or ArubaOS release version.</p> |
| 97685 | <p>Symptom: AirGroup did not adhere to the global RADIUS settings when the ip radius source-interface [loopback vlan] command was issued. The fix ensures that the global RADIUS configuration overrides the IP address used for sending AirGroup RADIUS requests.</p> <p>Scenario: This issue is not limited to any specific controller model or ArubaOS release version.</p> |
| 97771 | <p>Symptom: When the user tried to access Google® Chromecast the following error was displayed, selected device is no longer online. This issue is resolved by ensuring that the MAC multicast address for Simple Service Discovery Protocol (SSDP) packets is generated correctly.</p> <p>Scenario: This issue was observed if a user tried to connect to Chromecast when Airgroup service was enabled. This issue was caused because the controller was not receiving DLNA response from Chromecast for multicast DLNA queries, resulting in missing cache entries on the controller for DIAL service from Chromecast. This issue is observed in all controllers running ArubaOS 6.4 and later.</p> |
| 100002 | <p>Symptom: The CPPM server was flooded with AirGroup authorization requests from the controller. The fix ensures that the controller does not send AirGroup authorization requests if an AirGroup device changes its IP address.</p> <p>Scenario: This issue was observed on controllers running ArubaOS 6.3 and later. This issue is observed when a controller sends out RADIUS requests each time an AirGroup user changes the IP address.</p> |
| 102063 102258 102877 | <p>Symptom: The multicast Domain Name System (mDNS) process of AirGroup crashed and restarted on M3 controller. The logs for the event listed the reason for the crash as Nanny rebooted machine - low on free memory. Internal code changes are implemented to ensure the memory leak was removed.</p> <p>Scenario: A memory leak occurred every time the user sent a query and controller responded with the relevant mDNS records. This issue was observed in M3 controller running ArubaOS 6.3.1.7.</p> |

Air Management-IDS

Table 45: *Air Management-IDS Fixed Issues*

| Bug ID | Description |
|--------|---|
| 90630 | <p>Symptom: Log messages incorrectly warn of a Block ACK (BA) DoS attack from a valid client. Changes in the internal code have fixed this issue.</p> <p>Scenario: This issue was identified in a 6000 controller running ArubaOS 6.2.0.2 in a master-local topology.</p> |
| 96206 | <p>Symptom: The WMS module periodically failed to respond to SNMP requests when it removed monitored devices that were not in use. This issue is resolved by optimizing the WMS station check and AP removal process.</p> <p>Scenario: This issue occurred in large networks with many monitored devices, when the table size became large in the WMS module, and the WMS module failed to respond to the SNMP poll requests. This issue was not limited to any specific controller model or ArubaOS release version.</p> |

AP Regulatory

Table 46: *AP Regulatory Fixed Issues*

| Bug ID | Description |
|--------|--|
| 98303 | Symptom: Incorrect max EIRP value was displayed for AP-104. This issue is resolved by correcting the regulatory limit for EU countries. Scenario: This issue was observed in AP-104 access points running ArubaOS 6.3.1.x due to incorrect value defined for the regulatory limit for EU countries. |
| 98628 | Symptom: MaxEIRP for RAP-3WN/ RAP-3WNP was inconsistent due to wrong maximum tx-power setting. The fix ensures that the regulatory and hardware limits are correctly set. Scenario: This issue was observed when the value of configured tx-power was larger than the MaxEIRP. |

AP-Platform

Table 47: *AP-Platform Fixed Issues*

| Bug ID | Description |
|-------------------------|---|
| 95472 96239 | Symptom: When an AP was configured with a static IP address, the Link Aggregation Control Protocol (LACP) on AP-220 Series access points was not functional. This issue is resolved by initiating a LACP negotiation when an AP with a static IP is identified. Scenario: This issue was observed in AP-220 Series access points running ArubaOS 6.3.1.3 and 6.4.0.1 when configured with a static IP. |
| 95893 | Symptom: When an AP sent a DHCP request, it received an IP address 0.0.0.0 from the Preboot Execution Environment (PXE) server. Though the AP accepted this IP address, the AP could not communicate further and rebooted. The fix ensures that the PXE acknowledgment is ignored and the AP receives a valid IP address. Scenario: This issue was observed in deployment scenarios that have a DHCP server and multiple PXE servers. This issue was observed in APs running ArubaOS 6.3 or earlier. |
| 96051 96754 98008 | Symptom: AP-115 access points rebooted unexpectedly. This issue is resolved by adding a device queue status check before sending data to an Ethernet driver. Scenario: A crash occurred when the throughput was high on Ethernet connected to a 100/10M switch. This issue was observed in AP-114 and AP-115 access points running ArubaOS 6.3.x and later versions. |
| 97544 | Symptom: RAP-109 could not be used on un-restricted controllers that do not have Japan country code. This issue is resolved by mapping the country code in AP regulatory domain profile to the AP regulatory domain enforcement. Scenario: This issue was observed when the Instant AP with Japan Stock-Keeping Unit (SKU) was converted to Remote AP running ArubaOS 6.3.1.3. |
| 100586 | Symptom: AP-120 Series (802.11 a/b/g) access point models stopped working after upgrading to ArubaOS 6.4.x. Support for AP-120 Series (802.11 a/b/g) access point models are enabled in ArubaOS 6.4.x. Scenario: This issue was observed in AP-120 Series (802.11 a/b/g) access point models running ArubaOS 6.4.x. |

AP-Wireless

Table 48: *AP-Wireless Fixed Issues*

| Bug ID | Description |
|------------------|---|
| 83716 | <p>Symptom: Some of the IEEE 801.11g beacon transmit rates are not supported by AP-220 Series devices. This issue is resolved by allowing beacon transmit rates support for non-basic IEEE 801.11g.</p> <p>Scenario: This issue was triggered when non-basic IEEE 801.11g was not allowed to set down at brcm driver. This issue was observed in AP-220 Series devices and AP-270 Series running ArubaOS 6.3.x, 6.4.x or earlier versions.</p> |
| 88940 | <p>Symptom: A crash was observed on APs when the status of the channel was set inappropriately by the process handling the AP management. This issue is resolved by selecting the first channel of the current 802.11 band, using the auto-channel option.</p> <p>Scenario: This issue was observed when a standard RAP or CAP was configured at the Dynamic Frequency Selection (DFS) channel. This issue is observed in AP-70 connected to controllers running ArubaOS 6.3.1.2.</p> |
| 94482 96677 | <p>Symptom: An AP crashed due to an internal Watchdog timeout. This issue is resolved by reducing the wait time, and rebooting the AP to recover from that state.</p> <p>Scenario: This issue occurred within one of the reset functions in the Ethernet driver where there was a long wait, which exceeded the watchdog timeout, causing AP failure.</p> |
| 96751 | <p>Symptom: An AP continuously crashed and rebooted due to out of memory. Disabling wireless and rogue AP containment features in the Intrusion Detection System (IDS) profile resolved this issue.</p> <p>Scenario: This issue occurred when wireless and rogue AP containment features were enabled on the IDS profile. This issue was observed on AP-220 Series running ArubaOS 6.3.1.2 version.</p> |
| 97428 | <p>Symptom: Users were unable to access the network as the old DHCP route-cache entry was not modified by the new DHCP cache route on Aruba Remote APs (RAP). The fix ensures that the old route cache entry is replaced by the new route cache.</p> <p>Scenario: This issue was observed when IPs were assigned to clients through DHCP on RAP. This issue was observed in RAPs running ArubaOS 6.4.x.</p> |
| 99833 100559 | <p>Symptom: When more than 120 customers were connected in the bridge mode, broadcast packets were dropped and customers lost connectivity. This fix ensures that the broadcast packet handling is modified to resolve the issue.</p> <p>Scenario: This issue was observed when the frequency of customers trying to connect to the APs was high. This issue was observed in AP-225 connected to controllers running ArubaOS 6.3.1.2.</p> |
| 99922 | <p>Symptom: AP-220 Series access points displayed more than actual number of associated stations. When reclaiming the client data structures, there was inconsistency between driver and AP processes which is now resolved.</p> <p>Scenario: This issue was observed when the value of the parameter max-clients was set to 255 and the count of the associated and non-associated stations exceeded the maximum value. This issue was observed in AP-220 Series access points connected to controllers running ArubaOS 6.3.x and later versions.</p> |
| 100652 100731 | <p>Symptom: AP-225 access point was not transmitting multicast streams. This issue is resolved by fixing the accounting problem.</p> <p>Scenario: This issue was observed when the counter used to track the buffered multicast frames was not decremented when invalid frames in the buffers were discarded. When the counter reached the maximum outstanding multicast frames, no more multicast frames were allowed for transmission.</p> |

ARM

Table 49: *ARM Fixed Issues*

| Bug ID | Description |
|--------|--|
| 97585 | <p>Symptom: The show ap arm client-match history command displayed that a client was steered to a radio with less than -70 dBm. This was a display error. ARM log does not record the correct signal strength. The fix ensures that the ARM log always notes the signal strength that is used to make client match decision.</p> <p>Scenario: This issue was observed in controllers running ArubaOS 6.3.1.2 or later versions.</p> |

Authentication

Table 50: *Authentication Fixed Issues*

| Bug ID | Description |
|--------|---|
| 96492 | <p>Symptom: When 802.1X authentication was in progress, two key1 packets were sent out during key exchange. This issue is resolved by making code level changes to ensure that only one key1 packet is sent out during key exchange.</p> <p>Scenario: This issue was observed when machine authentication was enabled and when user authentication was processed. During this time if the machine-authentication details were found in the cache, key1 was sent out again for the second time. This issue is not limited to any specific controller model or ArubaOS release version.</p> |

Base OS Security

Table 51: *Base OS Security Fixed Issues*

| Bug ID | Description |
|----------------|---|
| 88563 96465 | <p>Symptom: Some cipher suites were not working when the operations were offloaded to hardware. This issue was resolved by disabling the cipher suites which were not working with the hardware engine.</p> <p>Scenario: This issue was observed during any crypto operation that uses Diffie-Hellman key exchange.</p> |
| 92817 | <p>Symptom: Wireless clients were blacklisted even when the rate of the IP Session did not exceed the threshold value set. This issue is resolved by increasing the storage of the threshold to 16 bits.</p> <p>Scenario: This issue was observed when the threshold of the IP Session rate was set to a value greater than 255. This issue was observed in controllers running ArubaOS 6.x.</p> |
| 95367 | <p>Symptom: Issuing the show rules <role-name> command from the controller's CLI resulted in an internal module (Authentication) crash. Ensuring that Access Control Lists (ACLs) are not configured with spaces in the code resolved the issue.</p> <p>Scenario: This issue was observed when a large number of ACL was configured with spaces in their names. This was not limited to any specific controller model or ArubaOS release version.</p> |
| 96755 | <p>Symptom: Wired 802.1X using EAP-MD5 authentication failed. This issue is resolved by the modifying the authentication code to allow the wired-clients that perform authentication using EAP-MD5 authentication framework.</p> <p>Scenario: This Issue was observed when wired clients connected directly either to the controller or to the Ethernet port of a Campus AP or Remote AP. This issue was not limited to a specific controller model or ArubaOS release version.</p> |

| Bug ID | Description |
|--------|--|
| 96980 | <p>Symptom: Customer faced connectivity issues with Pre-Shared Key (PSK), Mac Authentication, and VLAN Derivation as key1 packet was sent out twice. This issue is resolved by introducing serialized Mac Authentication and PSK.</p> <p>Scenario: This issue occurred when PSK and Mac Authentication were parallelly processed, but PSK was initiated before MAC Authentication VLAN update. This issue was observed in ArubaOS 6.3.1.1.</p> |
| 98492 | <p>Symptom: When the customer roamed from a demilitarized zone (DMZ) to an internal controller, the display showed wireless instead of wired. This issue is resolved by checking the tunnel through which the user is connected and changing the user to wired.</p> <p>Scenario: This issue was observed when the customer routed traffic from an internal controller to DMZ using the L2 GRE Tunnel. This issue was observed in 3600 controllers running ArubaOS 6.2.1.3.</p> |
| 100248 | <p>Symptom: The Authentication module crashed on a 7210 controller. This issue is resolved by adding preventive checks that prevent a wired user with zero MAC address, and by adding logs and error stats counters to identify occurrence of such crashes.</p> <p>Scenario: This issue was observed in a network where the Remote AP and a wired user were on the same controller. This issue is specific to 7210 controllers running ArubaOS 6.4.0.3.</p> |

Captive Portal

Table 52: *Captive Portal Fixed Issues*

| Bug ID | Description |
|--------|--|
| 98992 | <p>Symptom: After upgrading from ArubaOS 6.1.3.9 to ArubaOS 6.3.1.4, captive portal redirect was not sent, so CP Authentication could not be completed. This issue is resolved by introducing forward lookup mechanism to check if CP Authentication has been configured multiple times for the same client. If multiple CP Authentications are detected, they are redirected until the captive portal configuration is complete.</p> <p>Scenario: This issue was observed only when multiple CP Authentication configurations were created. This issue was observed in controllers running ArubaOS 6.4 and ArubaOS 6.3.1.3 or later versions.</p> |

Certificate Manager

Table 53: *Certificate Manager Fixed Issues*

| Bug ID | Description |
|--------|--|
| 98565 | <p>Symptom: When the customer tried to upload a CA Certificate, an error message was displayed - Not a CA certificate. This issue is resolved by making code level changes to check if CA is set to true when the certificate is uploaded.</p> <p>Scenario: This issue was observed when the customer tried to upload a RAP custom certificate.</p> |

Configuration

Table 54: *Configuration Fixed Issues*

| Bug ID | Description |
|-----------------------------------|--|
| 95535 95582 99934 100234 | <p>Symptom: The ACL configuration on the local controller went out of sync intermittently with the master controller. The fix ensures that when centralized licensing is enabled and if PEFNG license is installed, the ACL configuration associated with the license is not be changed even if the PEFNG license is not available temporarily.</p> <p>Scenario: This issue occurred when there was a change in licenses. This issue was observed in controllers running ArubaOS 6.3 in a master-local topology.</p> |

Controller-Datapath

Table 55: *Controller-Datapath Fixed Issues*

| Bug ID | Description |
|---|---|
| 84585 92227 92228 92883 94200 | <p>Symptom: Traffic failed to pass a network with heavy traffic (such as high levels of packet replication), when AES-CCM or another encryption/decryption modes were enabled. This issue is resolved by increasing the estimated time for packet processing, in the datapath.</p> <p>Scenario: This issue was identified on 7200 Series controller connected to 2000 APs when Gratuitous ARP messages were replicated and sent to clients.</p> <p>Duplicate Bugs: The following bug IDs have reported similar issues: 96860, 98380</p> |
| 93582 | <p>Symptom: A 7210 controller crashed. The logs for the event listed the reason for the crash as datapath timeout. Ensuring that the destination UDP port of the packet is PAPI port while processing Application Level Gateway (ALG) module resolved this issue.</p> <p>Scenario: This issue was observed in 7210 controllers running ArubaOS 6.3.1.0.</p> |
| 97223 | <p>Symptom: An L3 GRE tunnel between an Aruba controller and a Cisco device was not restored when there was a keep-alive failure. The fix ensures that Aruba and Cisco devices use the same protocol number in the GRE keep-alive packets.</p> <p>Scenario: This issue was observed when Aruba and Cisco devices used different protocol numbers in GRE keep-alive packets, and both the devices dropped the keep-alive packets sent by the other as the protocol number was unknown. This issue was not limited to any specific controller model and was observed in ArubaOS 6.4.x.</p> |
| 97434 | <p>Symptom: High volume of Address Resolution Protocol (ARPs) requests triggered an increase in datapath utilization, which resulted in service impact. This issue is resolved by introducing the arp and grat-arp parameters to drop or blacklist the clients that are sending excessive ARPs.</p> <p>Scenario: This issue was observed when a client excessively scanned and dropped the Internet Control Message Protocol (ICMP) packets. This issue was observed in a local M3 controller running ArubaOS 6.4.x, in a master-local topology.</p> |
| 98499 100392 100393 | <p>Symptom: Controllers crashed multiple times. The log files for the event listed the reason for the reboot as datapath exception.</p> <p>Scenario: When a wireless user generated encrypted wifi fragments, these fragments were sent to the security engine for decryption, which returned results that were out-of-order and some of them had decryption errors. The fix ensures that the wifi fragments out-of-order decryption errors are handled correctly.</p> |
| 98500 | <p>Symptom: A legacy platform controller crashed when it received more than three Aggregated Mac Service Data Unit (A-MSDU) fragments. To resolve this issue, a check is introduced in the controller to drop the packets when more than three A-MSDU fragments were received.</p> <p>Scenario: This issue was observed when a wireless client sent aggregated A-MSDU packets to the AP which was further fragmented to more than three packets and sent to the controller. This issue was specific to legacy platform controllers (6000 Series controllers platforms with XLR/XLS processors and 650 controllers) running ArubaOS 6.3 and 6.4.</p> |
| 99483 | <p>Symptom: When AMSDU-TX was enabled, one of the packets were incorrectly freed and another packets failed, which lead to double incarnation of the same buffer and the system crashed. The fix ensures that the buffers are freed correctly.</p> <p>Scenario: This issue was observed in controllers running ArubaOS 6.3 or later, and was not limited to any specific controller model</p> |
| 100084 | <p>Symptom: Unknown ARP (ARP without user entry in datapath) requests were flooded in RAP wired tunnels. This issue is resolved by changing the behavior of the unknown ARPs from flooding in RAP wired tunnels.</p> <p>Scenario: This issue was observed in all controllers running ArubaOS 6.3.1.6 or later.</p> |

Controller-Platform

Table 56: *Controller-Platform Fixed Issues*

| Bug ID | Description |
|---|--|
| 74428 88758 | <p>Symptom: On dual-media RJ45 ports 0/0/0 and 0/0/1, if the port speed was forced from/to 1 Gbps to/from 10/100 Mbps when traffic was flowing, traffic forwarding on the port stopped in an unintended manner. This issue is resolved by disabling the port to stop the traffic on the port before changing the speed and re-enabling the port after changing the speed.</p> <p>Scenario: This issue was observed in 7200 Series controllers running ArubaOS 6.2 in configurations or topologies where traffic is flowing.</p> |
| 76059 85289 92255 93467 93827 | <p>Symptom: A controller rebooted unexpectedly. The log files for the event listed the reason as Reboot Cause: kernel panic. The fix ensures that the httpd process resumes immediately after crashing.</p> <p>Scenario: This issue was seen in 7200 Series controller having a high density of IPv4 captive-portal users configured. This resulted in a high number of httpd processes running on the controller. This issue was observed in ArubaOS 6.2 or later versions.</p> <p>Duplicate Bugs: The following bug IDs have reported similar issues: 95431, 96293, 96791, 96827, 98196, 99287, 99360, 99362, 99472, 99568, 100857, 100858, 101476</p> |
| 91097 96923 | <p>Symptom: A local controller rebooted unexpectedly. The log files for the event listed the reason for the reboot as Mobility Processor update. The fix ensures that the controller does not reboot unexpectedly by making code level changes to the primary and secondary NOR flash boot partition.</p> <p>Scenario: This issue was observed in controllers running ArubaOS 6.1.3.9.</p> |
| 91541 94045 95079 | <p>Symptom: A controller rebooted due to low memory. Changes to the controller software fixed this issue.</p> <p>Scenario: This issue occurred when there was a continuous traffic inflow terminating on the control plane. This resulted in an internal component of the ArubaOS software to take up high memory. This issue was observed in 600 Series, 3000 Series, and M3 controllers running ArubaOS 6.1 or later versions.</p> |
| 94427 96347 97456 97468 97938 | <p>Symptom: An M3 controller rebooted unexpectedly. The log files for the event listed the reason for the reboot as User pushed reset error. The issue is resolved by removing the lock contention.</p> <p>Scenario: This issue was observed due to panic dump or SOS crash, which was a result of jumbo packet or packet corruption. This issue was observed in M3, 3200, 3400, and 3600 controllers, but was not limited to any specific ArubaOS release version.</p> <p>Duplicate Bugs: The following bug IDs have reported similar issues: 98425, 98656, 99448, 99919</p> |
| 96712 99920 | <p>Symptom: A local controller rebooted unexpectedly during terminal/ssh related operation. The log files for the event listed the reason for the reboot as Kernel panic. Internal changes in the ArubaOS code fixed this issue.</p> <p>Scenario: This issue was observed in 7240 controllers running ArubaOS 6.2.1.4.</p> |
| 97237 | <p>Symptom: A controller rebooted because of memory leak in the module that handles address, route, and interface related configurations and notifications on the system. This issue is resolved by fixing the memory leak in the flow.</p> <p>Scenario: Memory leak occurred when an interface or STP states changed frequently with PAPI error. This issue was observed on 651 controller running ArubaOS 6.2.1.6 or later.</p> |
| 97388 97658 98373 | <p>Symptom: Some access points went down when the controller to which they were connected rebooted. This issue is resolved by ensuring that the boot partition information is updated in the secondary bank of the controller.</p> <p>Scenario: This issue occurred when the controller rebooted due to a watchdog reset. This issue was not limited to any specific controller model or ArubaOS release version.</p> |

Table 56: *Controller-Platform Fixed Issues*

| Bug ID | Description |
|---|--|
| 97411 97816 98419 98686 98688 | <p>Symptom: Local handling Station Management (STM) and WLAN Management System (WMS) processes crashed, with 0x01 exit status. The fix ensures that during a specific table backup, the database does not get corrupted.</p> <p>Scenario: This issue occurs due to database table corruption. This issue was observed in controllers running ArubaOS 6.3 and ArubaOS 6.4.</p> |
| 95835 98034 98202 99342 | <p>Symptom: A controller stopped responding and rebooted. The log files for the event listed the reason as softwatchdog reset. This issue is resolved by removing the various race condition in the panic dump path and reimplementing the watchdog framework.</p> <p>Scenario: This issue was seen during datapath core dump. This issue was observed on 7200 Series controller running ArubaOS 6.3.1.2.</p> |
| 98873 100421 | <p>Symptom: A 650 controller crashed during reboot. The log files for the event listed the reason as address error on CPU4. This issue is resolved by reverting the sos_download sequence in rcS script.</p> <p>Scenario: This issue was observed in 650 controller running ArubaOS 6.2.1.5.</p> |
| 99106 | <p>Symptom: A large number of Only Bottom slots can arbitrate debug messages were generated and as a result the controller console was flooded with these redundant messages. The issue is fixed by disabling these redundant messages in the arbitration algorithm.</p> <p>Scenario: This issue was observed in M3 controllers and is not limited to any ArubaOS version.</p> |
| 99208 99210 99211 99212 99213 | <p>Symptom: A controller crashes due to memory leak in PIM after a long uptime (for example, 90 days). The fix ensures that there are no memory leaks in PIM module.</p> <p>Scenario: This issue is observed when IGMP snooping or proxy is enabled and users perform multicast streaming. This issue occurs when the user's DHCP pool range is too vast (more than 2 million addresses). This issue is not limited to any specific controller model or ArubaOS version.</p> |

DHCP

Table 57: *DHCP Fixed Issues*

| Bug ID | Description |
|----------------|---|
| 96117 96433 | <p>Symptom: Some wireless clients experienced delay in obtaining an IP address. This issue is fixed by disabling the DDNS (Dynamic Domain Name system) update logic within Dynamic Host Configuration Protocol (DHCP).</p> <p>Scenario: This issue occurred when the DHCP pool was configured with the domain name and the Domain Name System (DNS) server was configured on the controller, using ip name-server command. This resulted in DDNS update of the host and delayed the response for the DHCP request. This issue was not limited to any specific controller model or ArubaOS release version.</p> |

LLDP

Table 58: *LLDP Fixed Issues*

| Bug ID | Description |
|--------|---|
| 100439 | <p>Symptom: Clients were unable to disable the 802.3 TLV power in the AP LLDP configuration. This results in PoE allocation issue on the switches. The fix allows the customer to enable/disable the 802.3 power Type Length Value (TLV).</p> <p>Scenario: This issue was observed in 7210 controllers running ArubaOS 6.2.1.7.</p> |

Local Database

Table 59: *Local Database Fixed Issues*

| Bug ID | Description |
|--------|--|
| 95277 | <p>Symptom: Any RAP whitelist entry with special characters failed to synchronize with any controller, and synchronization failed for subsequent whitelist entries. The issue is resolved by correcting the handling of special characters for every field in RAP and CPSEC whitelist entries so that synchronization can happen properly.</p> <p>Scenario: This issue was observed where RAP and CPSEC whitelist entries are synchronized on controllers running ArubaOS 6.3.1.2.</p> |

IPsec

Table 60: *IPsec Fixed Issues*

| Bug ID | Description |
|-----------------|--|
| 97775 100139 | <p>Symptom: If a user entered a wrong password, the VIA application did not prompt thrice for a password retry. This issue is resolved by sending the XAUTH STATUS FAIL message to the VIA client before deleting the IKE/IPsec session of the VIA client.</p> <p>Scenario: This issue was observed in controllers running ArubaOS 6.2, 6.3, or 6.4. The issue was caused when the controller did not send XAUTH STATUS FAIL to the VIA client.</p> |
| 98901 | <p>Symptom: An internal process (ISAKMPD) crashed on the controller. This issue is fixed by properly allocating the Process Application Programming Interface (PAPI) message that is sent from ISAKMPD process to the Instant Access Point (IAP) manager.</p> <p>Scenario: This issue occurred when the IAPs terminated on the controller and established IKE/IPsec connections with the controller. This issue was more likely to happen on M3, 3600, and 3200 controller models than on 7200 Series controller models, and occurred on ArubaOS running 6.3 or later.</p> |
| 99675 | <p>Symptom: ISAKMPD process crashed on master controller when maximum number of RAP limit was reached and a new user had to be added. This issue is resolved by reworking the debug infra code to remove the tight loop.</p> <p>Scenario: This issue was observed when more than 2 supported RAPS terminated on a controller. This resulted in ISAKMPD process sitting in a tight loop.</p> |

Master-Redundancy

Table 61: *Master -Redundancy Fixed Issues*

| Bug ID | Description |
|--------|---|
| 98005 | <p>Symptom: After centralized licensing was enabled, the standby master displayed UPDATE REQUIRED message. This issue is resolved by ignoring the RAP bit when checking if a new license type has been added.</p> <p>Scenario: This issue was observed when the centralized licensing was enabled and the master controller had embedded AP licenses. This issue was not limited to a specific controller model but is observed in ArubaOS 6.3.1.3, when the master controller has embedded AP licenses.</p> |
| 98663 | <p>Symptom: Error messages were displayed when database synchronization was taking place in 600 Series controllers. This issue is resolved by removing support for iapmgr.</p> <p>Scenario: This issue was observed in 600 Series controllers. The issue is caused when the user upgrades to ArubaOS 6.3 and executes the write erase all command.</p> |

RADIUS

Table 62: *RADIUS Fixed Issues*

| Bug ID | Description |
|--------|---|
| 93578 | <p>Symptom: In the show auth-trace buff command output, the number of RADIUS request packets jumped from 127 to 65408. This issue is fixed by changing the data type of the variable used in the command output.</p> <p>Scenario: This issue occurred due to an incorrect value that was displayed in the command output. This issue was not limited to any specific controller model or ArubaOS version.</p> |
| 96038 | <p>Symptom: Sometimes, the user name was missing in the RADIUS accounting STOP messages sent from the controller. The fix ensures that a check is added for user entries with multiple IP addresses before revoking authentication.</p> <p>Scenario: This issue was observed when the controller revoked authentication for user entries with multiple IP addresses. This issue was not limited to any specific controller model or ArubaOS release version.</p> |

Remote AP

Table 63: *Remote AP Fixed Issues*

| Bug ID | Description |
|--------|--|
| 95572 | <p>Symptom: All clients, wired and wireless, connected to Remote AP (RAP), were unable to pass traffic locally with source NAT in split-tunnel forwarding mode. The fix ensures that the entries in the route-cache table are aged out correctly.</p> <p>Scenario: This issue was observed when the route-cache table reached the max size as the aging was not working. This issues was observed when the 3200XM controller was upgraded from ArubaOS 6.1.3.6 to ArubaOS 6.3.1.2.</p> |
| 97009 | <p>Symptom: A RAP failed to establish a PPPoE connection when the RAP's up-link port was VLAN tagged. The fix ensures that the RAP can establish a PPPoE connection with VLAN tag.</p> <p>Scenario: This issue was observed in RAPs running ArubaOS 6.3.1.3.</p> |
| 99466 | <p>Symptom: The output of the show iap table command incorrectly displayed the status of iap (branch) as UP with older tunnel inner ip, after the isakmpd process crashed. The fix ensures that the status of the iap(branch) is updated properly with the new inner ip.</p> <p>Scenario: This issue is observed in controllers running ArubaOS 6.3 and 6.4.</p> |

Role/VLAN Derivation

Table 64: *Role/VLAN Derivation Fixed Issues*

| Bug ID | Description |
|-------------------------------------|---|
| 89236 94936 96005 99978 | Symptom: Incorrect VLAN derived for mac-auth derived role-based VLAN. This issue is resolved by deriving the mac-auth derived role-based VLAN from the L2 user-role. Scenario: This issue was observed when a user entry existed, user entry was assigned to mac-auth derived role-based VLAN, and the client re-associated. A user was assigned to the default VLAN instead of the mac-auth derived role-based VLAN because mac-auth was skipped for the existing mac-authenticated user-entry. |
| 94423 | Symptom: There was a mismatch between the device id stored in the user table and the AP cache. The fix ensures that the information retrieved from show user command and device id cache display the information received in the first packet. Scenario: This issue was observed when the device id cache was not updated by the AP, but when the show user command was executed, the updated device id cache was displayed. This issue was not limited to any specific controller model or release version. |
| 97117 | Symptom: When the RADIUS server returned multiple Vendor Specific Attributes (VSAs), ArubaOS did not check these attributes or set user roles. This issue is fixed by verifying the list of attributes before matching them with the rules. Scenario: This issue was observed when a user tried to set a role using the VSA attributes that were returned from the RADIUS server. This issue was observed in 3400 controllers running ArubaOS 6.2.1.4. |
| 99745 100008 100198 100435 | Symptom: Role/VLAN derived from SDR and UDR were incorrect since they matched only the first rule. This issue is resolved by correcting the logical error in code to make sure role/VLAN derivation for SDR and UDR works correctly. Scenario: This issue occurred only when SDR and UDR was configured with multiple rules. |

Routing

Table 65: *Routing Fixed Issues*

| Bug ID | Description |
|--------|---|
| 94746 | Symptom: When the loopback IP address was used as the controller-ip, the controller was not reachable from a wired network after reboot for a specific configuration and timing. The controller was reachable only from the same subnet to which the controller's uplink belongs. This issue was not seen when a VLAN interface was used as the controller-ip. This issue is resolved by maintaining the correct sequence for appropriate execution of the two internal threads . Scenario: This issue was observed when two threads in an internal process tried to modify the kernel default route information and lost the sequence of execution. This issue was seen in 7200 Series controllers running ArubaOS 6.3.1.0. |

Startup Wizard

Table 66: *Startup Wizard Fixed Issues*

| Bug ID | Description |
|--------|--|
| 98110 | Symptom: Mobility Controller Setup Wizard page was stuck with Java script error when you clicked Next on the VLANs and IP Interfaces tab of the controller's WebUI. Changes in the internal XML code fixed this issue. Scenario: This issue was not limited to any specific controller model and was observed in ArubaOS 6.4.0.2. |
| 98159 | Symptom: Campus WLAN Wizard page was stuck in Role Assignment step when you clicked Next on the Authentication Server step of the controller's WebUI using Microsoft® Internet Explorer 10 or Internet Explorer 11. Changes in the internal XML code fixed this issue. Scenario: This issue is not limited to any specific controller model and is observed in ArubaOS 6.4.0.2. |

Station Management

Table 67: *Station Management Fixed Issues*

| Bug ID | Description |
|----------------|--|
| 86620 88646 | Symptom: The show ap association client-mac command showed client MAC addresses for clients that aged out beyond the idle timeout value. This issue is resolved by making code level changes to station table in the Station Management module. Scenario: This issue was not limited to any specific controller model or ArubaOS release version. |
| 96910 | Symptom: The SNMP query on the objects, wlanAPRxDataBytes64 and wlanAPTxDatBytes64 returned incorrect values for AP-225. This issue is resolved by making code level changes to the read function in the Broadcom® driver. Scenario: This issue was observed when the statistics in the Broadcom driver was parsed incorrectly. This issue was observed in AP-225 access points running ArubaOS 6.3.x and later versions. |

Voice

Table 68: *Voice Fixed Issues*

| Bug ID | Description |
|--------|--|
| 95566 | Symptom: When two parties made a VoIP call using Microsoft® Lync 2013, media classification running on the controller prioritized the media session with wrong DSCP values. The fix ensures that the WMM value is read from the TUNNEL Entry rather than the Bridge Entry, so that the value is correct. Scenario: The DSCP values configured under the ssid-profile did not take effect. This issue occurred when the initial VLAN and the assigned VLAN were different. This issue was observed on M3 controllers running ArubaOS 6.1.3.10. |

WebUI

Table 69: *WebUI Fixed Issues*

| Bug ID | Description |
|---------------------------|--|
| 94818 | <p>Symptom: AP Group name did not support special characters. With this fix, you can create an AP Group name with the following special characters: " / > < : } { + _) (* & ^ % \$ # @ ! [] ; , . /.</p> <p>Scenario: This issue was seen when you create an AP Group from the Configuration > WIRELESS > AP Configuration page of the controller's WebUI. This issue was not limited to any specific controller or release version.</p> |
| 95185 | <p>Symptom: Collecting the logs.tar with tech-support logs from the controller's WebUI failed with Error running report... Error: receiving data from CLI, interrupted system call error message. The fix ensures that the session is kept active till the logs are ready to be downloaded.</p> <p>Scenario: This issue was not seen under the following cases:</p> <ul style="list-style-type: none"> • Downloading the logs.tar without tech-support log from the WebUI. • Downloading the logs.tar with tech-support logs from the CLI. <p>This issue was observed in 7220 controller running ArubaOS 6.3.1.2.</p> |
| 98939 | <p>Symptom: The user was unable to access the Monitoring > Summary page on a controller GUI using Internet Explorer 9 (IE 9). This issue is resolved by implementing internal code changes that ensures the Web UI loads correctly.</p> <p>Scenario: This issue was observed when the controller was upgraded to ArubaOS 6.3.1.4-FIPS. This issue was caused by a missing DOCTYPE HTML code in the Monitoring > Summary page. Alternatively, the user can access the Monitoring > Summary page using Google Chrome or Mozilla Firefox. This issue is not limited to any specific controller model or ArubaOS version.</p> |
| 99356 | <p>Symptom: The WebUI incorrectly displayed that the interface was selected under IGMP in the Network > IP > IP Interface > Edit VLAN page even though a port channel was configured in the CLI. The fix ensures that the WebUI correctly displays the configured port channel when IGMP proxy is configured on a VLAN interface.</p> <p>Scenario: This issue was observed when the ip igmp proxy port-channel command was executed on a VLAN interface. This issue was observed in all the controller platforms.</p> |
| 99471 | <p>Symptom: The WebUI could not disable IGMP proxy when it was enabled under IGMP in the Network > IP > IP Interface > Edit VLAN page. The fix adds a new Enable IGMP checkbox under VLAN to enable or disable the IGMP options selected.</p> <p>Scenario: The WebUI did not allow disabling both IGMP snooping and IGMP proxy together once either of the radio buttons was selected. This issue was not limited to any specific controller model or ArubaOS version.</p> |
| 99961 100373 100771 | <p>Symptom: Remote AP settings were missing in the controller WebUI under the Configuration->Wireless->AP Installation > Provision page. The remote AP license check is removed to fix this issue.</p> <p>Scenario: This issue was observed in controllers running ArubaOS 6.3.1.6.</p> |
| 100051 | <p>Symptom: Banner text on login page of the controller's WebUI was incorrectly aligned. The fix ensures that the banner text is aligned correctly.</p> <p>Scenario: This issue was observed when a controller was upgraded to ArubaOS 6.3.x.</p> |

XML API

Table 70: XML API Fixed Issues

| Bug ID | Description |
|----------------|--|
| 97102 99101 | <p>Symptom: RADIUS accounting START message did not trigger for clients when a user was added using XML-API. To resolve this issue, the check-for-accounting parameter has been introduced in the Captive Portal configuration. This parameter helps in bypassing the check for Captive Portal profile role, by toggling between older versions of ArubaOS and ArubaOS 6.3 or later versions.</p> <p>Scenario: This issue was observed only when a user was added before the authentication was complete. This issue was not limited to any specific controller model or ArubaOS release version.</p> |

Resolved Issues in ArubaOS 6.4.0.3

The following issues were resolved in ArubaOS 6.4.0.3.

Base OS Security

Table 71: Base OS Security Fixed Issue

| Bug ID | Description |
|--------|---|
| 99070 | <p>Symptom: An Aruba controller's WebUI and captive-portal were vulnerable to an OpenSSL TLS heartbeat read overrun attack. For more information on this vulnerability, read the OpenSSL Security Advisory.</p> <p>The TLS heartbeat in the current OpenSSL version 1.0.1c is disabled so that any heartbeat request will be ignored by the controller. This change fixed the issue.</p> <p>Scenario: This issue was observed in controllers running ArubaOS 6.3 or later versions.</p> |

Resolved Issues in ArubaOS 6.4.0.2

The following issues were resolved in ArubaOS 6.4.0.2.

AirGroup

Table 72: AirGroup Fixed Issues

| Bug ID | Description |
|--------|--|
| 96675 | <p>Symptom: Local controllers handling multicast Domain Name System (mDNS) process crashed. To resolve this issue, the cache entries and memory used for the device that sends an mDNS response packet with a time-to-live (TTL) value as zero are cleared.</p> <p>Scenario: This issue was observed when the controller received mDNS response packets, and the value of TTL was set to zero. This issue was observed in ArubaOS 6.3, but was not specific to any controller model.</p> |

Application Monitoring (AMON)

Table 73: *AMON Fixed Issues*

| Bug ID | Description |
|--------|--|
| 94570 | Symptom: Incorrect roles were displayed in the WebUI dashboard for the clients connected to RAPs in split-tunnel mode. This issue was resolved by resetting the flag that populates the client role value in the dashboard. Scenario: This issue was not limited to any specific controller model or release version. |

AP-Platform

Table 74: *AP-Platform Fixed Issues*

| Bug ID | Description |
|-------------------------|--|
| 95893 | Symptom: When an AP sent a DHCP request, it received an IP address 0.0.0.0 from the Preboot Execution Environment (PXE) server. Though the AP accepted this IP address, the AP could not communicate further and rebooted. The fix ensures that the PXE acknowledgment is ignored and the AP receives a valid IP address. Scenario: This issue was observed in deployment scenarios that have a DHCP server and multiple PXE servers. This issue was observed in APs running ArubaOS 6.3 or earlier. |
| 96051 96754 98008 | Symptom: AP-115 access points rebooted unexpectedly. This issue is resolved by adding a device queue status check before sending data to an Ethernet driver. Scenario: A crash occurred when the throughput was high on Ethernet connected to a 100/10M switch. This issue was observed in AP-114 and AP-115 access points running ArubaOS 6.3.x and later versions. |
| 96239 95472 | Symptom: When an AP was configured with a static IP address, the Link Aggregation Control Protocol (LACP) on AP-220 Series access points was not functional. This issue is resolved by initiating a LACP negotiation when an AP with a static IP is identified. Scenario: This issue was observed in AP-220 Series access points running ArubaOS 6.3.1.3 and 6.4.0.1 when configured with a static IP. |
| 96913 | Symptom: When a controller was upgraded from ArubaOS 3.4.4.3 and above, or ArubaOS 5.0.x (5.0.3.1 or later), or ArubaOS 6.0.x (6.0.1.0 or later) to ArubaOS 6.4.0.1, APs failed to upgrade to ArubaOS 6.4.0.1. A defensive check is made in affected API so that PAPI messages which are smaller than PAPI header size are handled properly in ArubaOS 6.0.x compared to ArubaOS 5.0.x. Scenario: This issue was observed in APs running ArubaOS 3.x, or ArubaOS 5.0.x (5.0.3.1 or later) or ArubaOS 6.0.x (6.0.1.0 or later). APs running ArubaOS 6.1 and later versions are not impacted. |
| 97544 | Symptom: RAP-109 could not be used on un-restricted controllers that do not have Japan country code. This issue is resolved by mapping the country code in AP regulatory domain profile to the AP regulatory domain enforcement. Scenario: This issue was observed when the Instant AP with Japan Stock-Keeping Unit (SKU) was converted to Remote AP running ArubaOS 6.3.1.3. |

AP-Regulatory

Table 75: *AP-Regulatory Fixed Issues*

| Bug ID | Description |
|--------|---|
| 95759 | Symptom: RADAR detection and channel change events were observed in APs on Russia country code. The issue is fixed by correcting the country domain code for Russia. Scenario: This issue was not limited to any specific AP model or ArubaOS release version. |

AP-Wireless

Table 76: *AP-Wireless Fixed Issues*

| Bug ID | Description |
|--------|--|
| 86184 | Symptom: Wireless clients were unable to associate to an access point on the 5 GHz radio. This issue is resolved by making code level changes to ensure that an APs channel is changed after radar detection. Scenario: This issue was observed when a channel change in an access point failed after a Dynamic Frequency Selection (DFS) radar signature detection. This issue was observed in AP-125 running ArubaOS 6.1.x, 6.2.x, 6.3.x. |
| 96751 | Symptom: An AP continuously crashed and rebooted due to out of memory. Disabling wireless and rogue AP containment features in the Intrusion Detection System (IDS) profile resolved this issue. Scenario: This issue occurred when wireless and rogue AP containment features were enabled on the IDS profile. This issue was observed on AP-220 Series running ArubaOS 6.3.1.2 version. |
| 97818 | Symptom: Zebra® QL 420 Plus mobile printer did not associate with AP-220 Series access points. Improvements in the wireless driver of the AP in ArubaOS 6.4.0.2 resolved the issue. Scenario: This issue was observed in AP-220 Series access points running ArubaOS 6.3.1.2 or later versions. |

Authentication

Table 77: *Authentication Fixed Issues*

| Bug ID | Description |
|--------|---|
| 96285 | Symptom: The user was not assigned with the correct role when the XML API changed the user role. This issue is resolved by sending a notification to the Campus AP (CAP) in the bridge mode during External Captive Portal (ECP) event of role change. Scenario: This issue was observed when the client was connected to the CAP in the bridge mode. This issue was not limited to any specific controller model and occurred on ArubaOS running 6.3.1.2. |

Base OS Security

Table 78: *Base OS Security Fixed Issues*

| Bug ID | Description |
|--------|--|
| 93537 | Symptom: Wireless clients did not get a Dynamic Host Configuration (DHCP) IP. This issue is resolved by enabling both IP Mobility and MAC authentication, so that user gets an IP address even if the MAC authentication fails due to configuration error or connectivity issues. Scenario: This issue was observed when L3 mobility was configured on the controller and MAC authentication failed for the client, which caused mobile IP to drop packets from the client. This issue was not limited to any specific controller model or release version. |
| 96458 | Symptom: A controller rebooted with the reboot cause Nanny rebooted machine - low on free memory . This issue is resolved by freeing the memory that was leaking in the authentication module. Scenario: This issue was observed for VPN users when the cert-cn-lookup parameter was disabled under aaa authentication vpn profile. This issue was not limited to a specific controller model or release version. |
| 96755 | Symptom: Wired 802.1X using EAP-MD5 authentication failed. This issue is resolved by the modifying the authentication code to allow the wired-clients that perform authentication using EAP-MD5 authentication framework. Scenario: This Issue was observed when wired clients connected directly either to the controller or to the Ethernet port of a Campus AP or Remote AP. This issue was not limited to a specific controller model or release version. |

Captive Portal

Table 79: *Captive Portal Fixed Issues*

| Bug ID | Description |
|-------------------------|---|
| 92927 94414 97765 | Symptom: When Apple® iOS 7 clients tried to connect through the Captive Portal profile, the users were not redirected to the next page even after a successful authentication. A change in the redirect URL has fixed this issue. Scenario: This issue was observed only in clients using Apple iOS 7 devices. |

Controller-Datapath

Table 80: *Controller-Datapath Fixed Issues*

| Bug ID | Description |
|----------------|---|
| 92657 | Symptom: Although the prohibit-arp-spoofing parameter was disabled in firewall, clients were getting blacklisted with reason ARP spoofing . Controlling the action on ARP-spoofing only by the prohibit-arp-spoof parameter and on ip-spoofing only by the firewall prohibit-ip-spoof parameter fixed the issue. Scenario: This issue was not limited to a specific controller model or release version. |
| 93582 | Symptom: A7210 controller crashed. The logs for the event listed the reason for the crash as datapath timeout . Ensuring that the destination UDP port of the packet is PAPI port while processing Application Level Gateway (ALG) module resolved this issue. Scenario: This issue was observed in 7210 controllers running ArubaOS 6.3.1.0. |
| 95939 96156 | Symptom: The local controller crashed as buffer allocation requests were queued to a single processor that resulted in high CPU utilization. This issue is resolved by distributing allocation requests to different CPUs to balance the load across all processors. Scenario: This issue was observed in 7200 Series controllers running ArubaOS 6.3. |

Controller-Platform

Table 81: *Controller-Platform Fixed Issues*

| Bug ID | Description |
|---|--|
| 96420 88234 91172 93465 93913 | Symptom: A local controller rebooted unexpectedly. The log files for the event listed the reason for the reboot as Kernel Panic . This issue is resolved by making code level changes to handle chained buffer punts to the CPU. Scenario: This issue was observed when the local controller received an Aggregate MAC Service Data Unit (AMSDU) packet sent by the clients as fragmented multiple packets which triggered internal conditions. This issue was observed in 3600 controllers running ArubaOS 6.3.1.2. Duplicate Bugs: The following bug IDs have reported similar issues: 94754, 95664, 97384, 97761 |

IPSec

Table 82: *IPSec Fixed Issues*

| Bug ID | Description |
|----------------|---|
| 95634 97749 | Symptom: Site-to-Site IPsec VPN tunnels randomly lost connectivity on a7210 controller. This issue is resolved by making code level changes to ensure that the key length matches. Scenario: This issue was observed when there were 500 or more remote sites terminating IPsec VPN tunnels on a7210 controller running ArubaOS 6.3.1.2. |

Mobility

Table 83: *Mobility Fixed Issues*

| Bug ID | Description |
|----------------------------------|---|
| 83927 | Symptom: When the primary HA went down, the alternate HA did not become the home agent for a roaming client although the auth-sta-roam parameter was disabled. This issue is resolved by creating a user-entry on the alternate HA using user information from the primary HA when the primary HA goes down. Scenario: This issue was observed on controllers running ArubaOS 6.3 in a setup containing an HA, FA, and an alternate HA with L3 mobility enabled and the auth-sta-roam parameter disabled. |
| 96207 96214 96222 96555 | Symptom: The client did not receive an IP address through DHCP, and could not pass traffic when L3 mobility was enabled on the controller. This issue is resolved by clearing the state machine of the affected client. Scenario: This issue was observed when the client roamed from a Virtual AP (VAP) in which the mobile-ip parameter was enabled to a VAP in which the mobile-ip parameter was disabled. This issue was observed in ArubaOS 6.3 and later versions, but was not limited to a specific controller model. |

RADIUS

Table 84: *RADIUS Fixed Issues*

| Bug ID | Description |
|--------|--|
| 96038 | Symptom: Sometimes, the user name was missing in the RADIUS accounting STOP messages sent from the controller. The fix ensures that a check is added for user entries with multiple IP addresses before revoking authentication. Scenario: This issue was observed when the controller revoked authentication for user entries with multiple IP addresses. This issue was not limited to any specific controller model or release version. |

Remote AP

Table 85: *Remote AP Fixed Issues*

| Bug ID | Description |
|--------|---|
| 97009 | Symptom: A RAP failed to establish a PPPoE connection when the RAP's up-link port was VLAN tagged. The fix ensures that the RAP can establish a PPPoE connection with VLAN tag. Scenario: This issue was observed in RAPs running ArubaOS 6.3.1.3. |

Station Management

Table 86: *Station Management Fixed Issues*

| Bug ID | Description |
|----------------|--|
| 86620 88646 | Symptom: The show ap association client-mac command showed client MAC addresses for clients that aged out beyond the idle timeout value. This issue is resolved by making code level changes to station table in the STM module. Scenario: This issue was not limited to a specific controller or ArubaOS release version. |

Voice

Table 87: *Voice Fixed Issues*

| Bug ID | Description |
|----------------|--|
| 94038 94600 | Symptom: The show voice call-cdrs and show voice client-status commands displayed incorrect state transitions for consulted, transfer, and speaker announced call scenarios. The fix ensures the state transitions for New Office Environment (NOE) application layer gateway. Scenario: This issue was observed in an NOE deployed voice environment with controllers running ArubaOS 6.1 or later versions. |

WebUI

Table 88: *WebUI Fixed Issues*

| Bug ID | Description |
|-------------------------|---|
| 68464 94529 94961 | Symptom: The user was forced out of a WebUI session with the Session is invalid message. This issue is resolved by fixing the timing issue for the exact session ID from cookies in the https request. Scenario: This issue was observed when a web page of the parent domain name was accessed previously from the same browser. This issue was not limited to any specific controller model or release version. |
| 96465 | Symptom: Some cipher suites were not working when the operations were offloaded to hardware. This issue was resolved by disabling the cipher suites which were not working with the hardware engine. Symptom: This issue was observed during any crypto operation that uses DH key exchange. |
| 94818 | Symptom: AP Group name did not support special characters. With this fix, you can create an AP Group name with the following special characters: " / > < : } { + _) (* & ^ % \$ # @ ! [] ; , . / . Scenario: This issue was seen when you create an AP Group from the Configuration > WIRELESS > AP Configuration page of the controller's WebUI. This issue was not limited to any specific controller or release version. |

Resolved Issues in ArubaOS 6.4.0.1

The following issues were resolved in ArubaOS 6.4.0.1:

PhoneHome

Table 89: *PhoneHome Fixed Issues*

| Bug ID | Description |
|--------|--|
| 96789 | Symptom: Starting with ArubaOS 6.4.0.1, PhoneHome automatic reporting is disabled by default. This is a change in behavior from ArubaOS 6.4.0.0, as this feature was automatically enabled when the controller upgraded to ArubaOS 6.4.0.0. Scenario: This change in behavior impacts controllers upgrading to ArubaOS 6.4.0.1. |

Resolved Issues in ArubaOS 6.4.0.0

The following issues were resolved in ArubaOS 6.4.0.0.

802.1X

Table 90: *802.1X Fixed Issues*

| Bug ID | Description |
|--------|---|
| 89106 | <p>Symptom: A configured CLASS attribute was missing from the accounting messages sent from the RADIUS server to clients when previously idle clients reconnected to the network.</p> <p>Scenario: This issue occurred in a deployment using RADIUS accounting, where the RADIUS server pushed CLASS attributes in the access-accept messages for 802.1X authentication. When an idle user timed out from the network, ArubaOS deleted the CLASS attribute for the user along with rest of the user data.</p> <p>This issue is resolved with the introduction of the delete-keycache parameter in the 802.1X authentication profile, which, when enabled, deletes the user keycache when the client's user entries get deleted. This forces the client to complete a full 802.1X authentication process when the client reconnects after an idle timeout, so the CLASS attributes are again be sent by the RADIUS servers.</p> |
| 92564 | <p>Symptom: Clients experienced authentication failure when they used 802.1 x authentication. This issue is resolved by increasing the stack size.</p> <p>Scenario: The issue occurred due to stack overflow, which caused memory corruption. This issue was observed in 600 Series controllers and 3000 Series controllers running ArubaOS 6.1 and 6.2.</p> |

AirGroup

Table 91: *AirGroup Fixed Issues*

| Bug ID | Description |
|----------------|--|
| 88522 92368 | <p>Symptom: The multicast Domain Name System (mDNS) process of AirGroup crashed and restarted on a controller. This issue is resolved by blocking the memory leak to ensure that the controller is not crashing when the maximum number of servers and users supported on each platform is exceeded.</p> <p>Scenario: This issue was triggered when the number of AirGroup users exceeded the limit specified on a platform. This issue was observed in the controllers except 600 Series controllers running earlier versions of ArubaOS 6.4.</p> |

Air Management-IDS

Table 92: *Air Management-IDS Fixed Issues*

| Bug ID | Description |
|--------|---|
| 84148 | <p>Symptom: The show wms client command took a long time to return output. This issue is fixed by retrieving wms client information from the in-memory data structures, instead of sending queries to the database.</p> <p>Scenario: This issue occurred when the show wms client command was executed. This issue was not limited to any specific controller model or release version.</p> |
| 90330 | <p>Symptom: An adhoc AP was classified to be manually contained, but it would not be contained unless the protect from adhoc feature was also enabled. This issue is resolved by changes that ensure an adhoc AP marked for containment is correctly contained.</p> <p>Scenario: This issue was observed in controllers running ArubaOS 6.2 or later.</p> |
| 92070 | <p>Symptom: The age field in the Real-Time Location System (RTLS) station report sent by an AP was sometimes reset although the station was no longer being heard by the AP.</p> <p>Scenario: This issue occurred when the detecting AP can no longer hear frames from the station, but it can still hear frames sent by other APs to the station. This issue could occur on a controller running ArubaOS 6.1 or later.</p> |

Table 92: *Air Management-IDS Fixed Issues*

| Bug ID | Description |
|--------|--|
| 93912 | <p>Symptom: Issuing the show wms client probe command did not return any output and instead it displayed the WMS module busy message after a timeout period. Executing the command with the MAC address of the client fixed this issue.</p> <p>Scenario: This issue is observed when there was a large number of entries in the WLAN Management System (WMS) table. This issue is not limited to any specific controller model or ArubaOS version.</p> |

AP-Datapath

Table 93: *AP-Datapath Fixed Issues*

| Bug ID | Description |
|--------|--|
| 90645 | <p>Symptom: The show datapath session ap-name command output did not display ap-name option. The command output is now displayed correctly even if the ap-name parameter is used.</p> <p>Scenario: This issue was observed in controllers running ArubaOS 6.2.1.3 and was not limited to any specific controller model.</p> |
| 94067 | <p>Symptom: The VLAN in the wired AP is different from the AP's native VLAN.</p> <p>Scenario: This issue occurred on the AP-93H device connected to controllers running any ArubaOS version. This issue occurred because the wired driver did not support the extra two bytes used by the internal switch chip.</p> |

AP-Platform

Table 94: *AP-Platform Fixed Issues*

| Bug ID | Description |
|--------|---|
| 86096 | <p>Symptom: When multiple DNS servers were configured in a local RAP DHCP pool, only the first server in the DNS server list was available to the DHCP client.</p> <p>Scenario: This issue was observed in RAPs that were configured to use a local DHCP server and were running ArubaOS 6.2 or 6.3. This issue occurred due to incorrect handling of the DNS servers configured by SAPD.</p> |
| 86112 | <p>Symptom: The APs went to an inactive state. Changes in the internal code fixed this issue.</p> <p>Scenario: This issue was observed when the named-vlan parameter was configured in wlan virtual-ap <name> command and when all the VLAN IDs were greater than 4064. This issue was not limited to any specific controller model or ArubaOS version.</p> |
| 87775 | <p>Symptom: A Remote AP (RAP) crashed due to incorrect watchdog feeding. The issue is resolved by ensuring that the hardware watchdog feeding is done periodically.</p> <p>Scenario: This issue was observed in RAP-5WN and AP-120 Series access points running ArubaOS 6.3 or earlier versions when there was a high traffic flow in the network.</p> |
| 87857 | <p>Symptom: Fragmented configuration packets sent from the controller to the AP can cause the AP to come up with the "D:" (dirty) flag. Improvements to how ArubaOS handles out-of-order packets resolve this issue.</p> <p>Scenario: This issue is triggered by network congestion or breaks in the connection between the controller and AP.</p> |

Table 94: *AP-Platform Fixed Issues*

| Bug ID | Description |
|---|---|
| 88288 88568 89040 89135 89137 | <p>Symptom: 802.11n-capable APs unexpectedly stopped responding and rebooted. Log files for the event listed the reason for the crash as kernel panic or kernel page fault. This issue was resolved by improvements to the wireless drivers in ArubaOS 6.3.1.1.</p> <p>Scenario: This issue occurred on AP-125, AP-135, and AP-105 access points running ArubaOS 6.3.0.1.</p> <p>Duplicate Bugs: The following bug IDs have reported similar issues: 89252, 89254, 89255, 90021, 90028, 90495, 90604, 91016, 91392, 91393, 91755, 92585, 93336</p> |
| 88389 89882 90175 90332 | <p>Symptom: 802.11n-capable access points unexpectedly rebooted. The log files for the event listed the reason for the reboot as kernel page fault. Improvements in the wireless driver of the AP resolved this issue.</p> <p>Scenario: This issue was observed when an 802.11n-capable campus AP was in bridge forwarding mode and there was a connectivity issue between the AP and the controller. This issue was observed in 802.11n-capable access points running any version of ArubaOS.</p> |
| 88504 92678 | <p>Symptom: No output was displayed when the show ap config ap-group <ap-group> command was executed. Increasing the buffer size of SAPM (an AP management module in STM) resolved this issue.</p> <p>Scenario: This issue was observed on controllers running ArubaOS 6.3.x.x.</p> |
| 88813 89594 | <p>Symptom: The show ap allowed-max-EIRP command displayed incorrect information for AP-220 Series access points. This display issue is resolved by increasing the buffer size that stores Effective Isotropic Radiated Power (EIRP) information.</p> <p>Scenario: This issue was observed in 3200 Series controllers and 3400 Series controllers running ArubaOS 6.3.x.</p> |
| 89016 | <p>Symptom: The SNMP OID wlanStaAccessPointESSID had no value when a client roamed from a down AP to an active AP. Improvements to internal processes that manage layer-2 roaming resolve this issue.</p> <p>Scenario: This issue was observed when clients roamed between APs running ArubaOS 6.2.</p> |
| 89041 | <p>Symptom: A 802.11n-capable access point unexpectedly rebooted or failed to respond. This issue is resolved by improvements to the wireless drivers in ArubaOS 6.3.1.1.</p> <p>Scenario: This issue was observed when a client disconnected from the network. The issue occurred on 802.11n access points running ArubaOS 6.3.0.1.</p> |
| 89042 | <p>Symptom: An access point crashed and rebooted frequently. The log files for the event listed the reason for the crash as kernel panic. This issue is resolved by improvements to the wireless drivers in ArubaOS 6.3.1.1.</p> <p>Scenario: This issue was observed in 802.11n access points running ArubaOS 6.3.0.1.</p> |
| 89043 89054 89045 | <p>Symptom: 802.11n-capable access points unexpectedly rebooted or failed to respond. This issue is resolved by improvements to the wireless drivers in ArubaOS 6.3.1.1.</p> <p>Scenario: This issue was observed on 802.11n-capable access points running ArubaOS 6.3.0.1.</p> |
| 89514 92163 93504 | <p>Symptom: AP-220 Series access point rebooted repeatedly when connected to a Power over Ethernet (PoE) switch without storing a reboot reason code in the flash memory of the AP. Design changes to the AP-220 Series access point code resolved the issue.</p> <p>Scenario: This issue was observed on AP-220 Series access points running ArubaOS 6.3.x or later versions.</p> |
| 89691 94047 | <p>Symptom: APs stopped responding and rebooted. The log files for the event listed the reason for the crash as kernel page fault. A change in the route cache has fixed this issue.</p> <p>Scenario: This issue occurred when the deletion of the route cache was interrupted. This issue was not limited to any specific controller model or release version.</p> |

Table 94: AP-Platform Fixed Issues

| Bug ID | Description |
|---|---|
| 90854 | <p>Symptom: On multiport APs (such the AP-93H), the APs bridge priority was configured as 8000 by default. This caused the AP to become a root bridge, when connected to a switch, and the AP became slow.</p> <p>Scenario: Starting in ArubaOS 6.4, the default value has been set to 61440 (0xF000), which avoids this issue.</p> |
| 91803 | <p>Symptom: An AP-120 Series controller failed unexpectedly.</p> <p>Scenario: This issue occurred on an AP-120 Series controller running on ArubaOS 6.3.10. It was due to the AP's memory is low due to heavy traffic or many clients.</p> |
| 88793 91804 92194 92195 92700 | <p>Symptom: APs stopped responding and crashed due to a higher utilization of memory caused by the client traffic. A change in the AP memory management resolved this issue.</p> <p>Scenario: This issue was observed in ArubaOS 6.2 and later versions, but was not limited to a specific controller model.</p> <p>Duplicate Bugs: The following bug IDs have reported similar issues: 92749, 93080, 93140, 93695, 93798, 93845, 93997</p> |
| 91820 | <p>Symptom: An AP crashed and rebooted frequently and the log file for the event listed the reason for the reboot as Kernel Panic. Updates to the wireless driver fixed this issue.</p> <p>Scenario: This issue occurred while receiving and freeing the buffer memory. This issue was observed in AP-135 access points running ArubaOS 6.3.1.0.</p> |
| 91937 | <p>Symptom: AP-92 and AP-93 access points were unable to come up with ArubaOS 6.3.x.x-FIPS. ArubaOS 6.3.x.x-FIPS now supports AP-92 and AP-93 access points.</p> <p>Scenario: When upgrading to ArubaOS 6.3.x.x-FIPS, the image size was too big to fit into AP-92's or AP-93's 8 MB flash, and hence was rejecting these access points to come up although these access points required to be supported with 16 MB flash.</p> <p>NOTE: Due to the infrastructure limitation, to support 16 MB flash, the code block for 8 MB flash had to be removed as well. So, AP-92 and AP-93 access points with 8 MB flash will also come up with ArubaOS 6.3.x.x-FIPS but it is not supported. Only the AP-92 and AP-93 access points with 16 MB flash are supported with ArubaOS 6.3.x.x-FIPS.</p> |
| 91963 | <p>Symptom: An AP rebootstrapped with the Wrong cookie in request error after a failover from one controller to another. This issue is fixed by enhancements to drop the error message if an AP detected a cookie mismatch when the error message came from a different controller than current the LMS.</p> <p>Scenario: This issue occurred after a failover of an AP from one controller to another, and when the AP received the messages from old controller and incorrectly identified as a cookie mismatch. This issue was observed in controllers in a master-local topology with an LMS and a backup LMS configured.</p> |
| 92245 | <p>Symptom: An AP did not respond with "aruba_valid_rx_sig: Freed packet on list at ath_rx_tasklet+0x138/0x2880....." message and needed a manual power cycle to restore the normal status. This issue is resolved by improvements to the wireless drivers in ArubaOS 6.4.</p> <p>Scenario: This issue occurred when the buffer was corrupted in wireless driver. This issue was observed in AP-125 model access points associated to controllers running ArubaOS 6.3.1.</p> |
| 92348 | <p>Symptom: Upstream traffic flow was interrupted and caused IP connectivity issues on MAC OS clients. This issue is fixed by setting the maximum number of MAC service data units (MSDUs) in one aggregate-MSDU (A-MSDU) to 2 and disabling the de-aggregation of AMSDU for tunnel mode VAP.</p> <p>Scenario: This issue occurred when the maximum number of MSDUs in one A-MSDU was set to 3, which was not supported in Broadcom driver. This issue was observed in MacBook Air clients associated with AP-225 access points running ArubaOS 6.3.1.0.</p> |
| 92572 | <p>Symptom: APs stopped responding and crashed due to a higher utilization of memory caused by the client traffic. A change in the AP memory management has resolved this issue.</p> <p>Scenario: This issue was observed in ArubaOS 6.2 and later versions, but is not specific to any controller model.</p> |

Table 94: *AP-Platform Fixed Issues*

| Bug ID | Description |
|---|---|
| 93012 95172 | Symptom: Sometimes, a low voice call quality was observed on the clients. This issue is resolved by suspending any off-channel AP operation and ensuring that the voice calls are given higher priority. Scenario: This issue was observed in AP-225 connected to controllers running ArubaOS 6.3.1.0 and earlier versions. |
| 93067 | Symptom: The authorization for users was unexpectedly revoked and the show ap client trail-info CLI command displayed the reason as Ptk Challenge Failed . Sending the Extensible Authentication Protocol over LAN (EAPoL) packets as best effort traffic instead of voice traffic resolved this issue. Scenario: This issue was observed in AP-220 Series access points running ArubaOS 6.3.1.1 when the virtual AP is configured with WPA-802.1X-AES encryption. |
| 93715 93380 93494 93687 93744 | Symptom: An unexpected reboot of an AP-220 Series AP occurred due to a kernel panic. Internal software changes resolved this issue. Scenario: This reboot was triggered by VAP deletion and can occur upon mode change when all VAPs are deleted. The crash was caused because the PCI device is put to sleep when all the VAPs are deleted but ArubaOS accessed the PCI device before it woke up. This issue was limited to AP-220 Series APs running any version of ArubaOS. Duplicate Bugs: The following bug IDs have reported similar issues: 93780, 93904, 94068, 94102, 94124, 94146, 94166, 94192, 94193, 94196, 94258, 94371, 94373, 94422, 94455, 94540, 94564, 94763, 94843, 94864, 94893, 94917, 94918, 94927, 94937, 94956, 94988, 95010, 95011, 95144, 95189, 95259, 95293, 95619 |
| 94189 | Symptom: The enet1 interface of AP-135 did not power up when connected to a data switch. Starting with ArubaOS 6.4, the AP-130 Series supports full functionality when powered by an 802.3af Power over Ethernet (PoE) power source. Scenario: The issue was observed when the AP was connected to an 802.3af PoE power source. This issue was observed in AP-135 access points, but is not specific to any version of ArubaOS. |
| 94279 94720 | Symptom: A regulatory mismatch was observed on non-US controllers after an IAP was converted to a controller based AP. This issue is resolved by adding a new rule to verify the RW domain and accept RW APs on non-US controllers. Scenario: This issue was observed in IAP-224, IAP-225-RW, IAP-114, and IAP-115-RW. |
| 94456 | Symptom: Users observed AP reboot issues with two source mac addresses from the same port. This issue is fixed by not allowing ICMPv6 packets before Ethernet 1 is bonded even when it is UP. Scenario: This issue occurred when Ethernet 1 acted as uplink on an AP and the first ICMPv6 packet was sent with source MAC address of Ethernet 1. However, the successive ICMPv6 packets were sent with the source MAC of Ethernet 0 and caused AP reboot. This issue was not limited to any AP, controller models, and ArubaOS release version. |

AP Regulatory

Table 95: *AP Regulatory Fixed Issues*

| Bug ID | Description |
|--------|---|
| 86764 | Symptom: The output of the show ap allowed channels command incorrectly displayed that 5 GHz channels were supported on AP-68 and AP-68P. This issue is resolved by modifying the allowed channel list for AP-68 and AP-68P. Scenario: This issue was observed in AP-68 and AP-68P running ArubaOS versions 6.1.x, 6.2.x, or 6.3. |
| 90995 | Symptom: The Effective Isotropic Radiated Power (EIRP) was inconsistent and in some instances greater than the MaxEIRP, for HT20 and W52. This issue is resolved by updating the algorithm to consider the maximum EIRP for all modulation schemes. Scenario: This issue was observed in M3 controllers running ArubaOS 6.1.3.6. |

AP-Wireless

Table 96: *AP-Wireless Fixed Issues*

| Bug ID | Description |
|---|--|
| 67847 69062 69346 71530 74352 | <p>Symptom: APs unexpectedly rebooted and the log files listed the reason for reboot as Data BUS error. A change in the exception handling module has fixed this issue.</p> <p>Scenario: This issue was observed in AP-120 Series and AP-68P devices connected to controllers running ArubaOS 6.3.1.2.</p> <p>Duplicate Bugs: The following bug IDs have reported similar issues: 74687, 74792, 75212, 75792, 75944, 76142, 76217, 76715, 77273, 77275, 78118, 80735, 82147, 83242, 83243, 83244, 83624, 83833, 84170, 84339, 84511, 85015, 85054, 85086, 85367, 85959, 88515, 89136, 89253, 89256, 89816, 90603, 91084, 92871, 92877, 92878, 92879, 93923</p> |
| 69424 71334 74646 75248 75874 | <p>Symptom: When upgraded to ArubaOS 6.2, AP-125 crashed and rebooted. Reallocating the ArubaOS loading address in memory fixed the issue.</p> <p>Scenario: This issue was observed when upgrading to ArubaOS 6.2 from ArubaOS 6.1.3.2 and later in any deployment with an AP-125.</p> <p>Duplicate Bugs: The following bug IDs have reported similar issues: 78978, 78981, 79891, 80054, 85753, 87250, 87360, 88619, 88620, 88989, 89537, 91689, 92641, 92975, 93079, 93455, 93811, 91689</p> |
| 86398 | <p>Symptom: The output of the show ap debug system-status command showed an unexpectedly large increase in the buffers in use for queue 8. Changes in how unfinished frames are queued prevents an error that allowed this counter to increment more than once per frame.</p> <p>Scenario: This occurred in AP-135 and AP-115 access points running ArubaOS 6.3.x.x, and managing multicast traffic without Dynamic Multicast Optimization (DMO).</p> |
| 86456 | <p>Symptom: A controller running ArubaOS 6.3 with an AP-125 running as a RAP rebooted unexpectedly. This was caused when the AP received a BC/MC auth frame and failed.</p> <p>Scenario: This issue occurred on an AP-125 access point running ArubaOS 6.3.</p> |
| 86584 | <p>Symptom: The AP-225 did not support prioritization for multicast traffic.</p> <p>Scenario: This issue was observed on the AP-220 Series running ArubaOS 6.3.x.</p> |
| 88282 | <p>Symptom: AP-220 Series access points running ArubaOS 6.3.0.1 stopped responding and rebooted. The log files for the event listed the reason for the crash as kernel panic: Fatal exception. ArubaOS memory improvements resolve this issue.</p> <p>Scenario: This issue occurred in a master-local 7200 Series controller topology where the AP-220 Series AP terminated on both the controllers in campus mode.</p> |
| 88328 | <p>Symptom: Wireless clients experienced packet loss when connecting to remote AP that was in bridge mode. The fix ensures that some buffer is reserved for transmitting unicast traffic.</p> <p>Scenario: This issue was observed in AP-105 running ArubaOS 6.1.3.8 when there was a huge multicast or broadcast traffic in the network.</p> |
| 88385 94033 | <p>Symptom: Bridge mode users (802.1x and PSK) are randomly unable to associate to a RAP. Adding reference count for messages between authentication and Station management processes to avoid incorrect order of messages resolved this issue.</p> <p>Scenario: This issue occurred because of the incorrect order of messages between authentication and station management processes. This issue was observed in controllers running ArubaOS 6.3.0.1 or later.</p> |
| 88741 | <p>Symptom: Throughput degradation was observed on the AP-225.</p> <p>Scenario: This issue was caused by an internal ArubaOS malfunction and was observed only in AP-225.</p> |

Table 96: *AP-Wireless Fixed Issues*

| Bug ID | Description |
|---|--|
| 88771 88772 91086 | <p>Symptom: 802.11n capable access points stopped responding and rebooted. The log files for the event listed the reason for the crash as kernel page fault. This issue was resolved by improvements to the wireless drivers in ArubaOS 6.3.1.1.</p> <p>Scenario: This issue was observed only in 802.11n capable access points running ArubaOS 6.3.0.1.</p> |
| 88827 93771 | <p>Symptom: An AP stopped responding and reset. Log files listed the reason for the event as ath_bstuck_tasklet: Radio 1 stuck beacon; resetting. Changes in the ArubaOS 6.4 channel change and radio reset routines prevent this error.</p> <p>Scenario: This issue occurred in an AP-125 running ArubaOS 6.2.1.3, and was not associated with any controller model.</p> |
| 89442 93804 | <p>Symptom: The AP-220 Series controllers crashed frequently. Log files listed the reason for the event as Kernel Panic: Unable to handle kernel paging request.</p> <p>Scenario: This issue occurred when the radio mode was altered between Monitor and Infrastructure. This issue was observed only in AP-220 Series controllers running ArubaOS 6.3.1.2.</p> |
| 88631 88044 88569 88843 89044 | <p>Symptom: An access point stopped responding and continuously rebooted. Improvements in the wireless driver of the AP fixed this issue.</p> <p>Scenario: This issue was observed in AP-220 Series running ArubaOS 6.3.0.1 when clients disconnected from the network.</p> <p>Duplicate Bugs: The following bug IDs have reported similar issues: 89046, 89053, 89058, 89325, 89326 , 89811 , 89901 , 90890, 92076, 92336, 92786, 93335</p> |
| 89460 | <p>Symptom: When APs used adjacent DFS channels, the AP-135 falsely detected RADAR and exhausted all DFS channels. If no non-DFS were enabled, the AP stopped responding to clients.</p> <p>Scenario: This issue was observed in an AP-135 running ArubaOS 6.3.x and 6.2.x. It was caused when APs used adjacent DFS channels.</p> |
| 89735 89970 90572 91140 91560 | <p>Symptom: The Ethernet interface of an 802.11ac capable AP restarted frequently. Changes in the internal code fixed this issue.</p> <p>Scenario: This issue was observed in AP-220 Series access points running ArubaOS 6.3.1.0 and later versions.</p> <p>Duplicate Bugs: The following bug IDs have reported similar issues: 91620, 92017, 92428, 93373</p> |
| 90960 | <p>Symptom: Microsoft® Surface Pro and Surface RT clients were unable to acquire an IP address or correctly populate the ARP table with a MAC address when connecting to an AP using 20 MHz channels on 2.4 GHz or 5 GHz radios. This issue is resolved by channel scanning improvements to APs in 20 MHz mode.</p> <p>Scenario: This issue was triggered when Microsoft Surface clients running Windows 8 or Windows 8.1 connected to 20 MHz APs running ArubaOS 6.1.3.8.</p> |
| 91192 | <p>Symptom: Poor performance was observed in clients connecting to an AP due to non-WiFi interference. Implementing the Cell-Size-Reduction feature in AP-220 Series along with deauthorizing clients when they are about to go out of the desired cell range resolved this issue.</p> <p>Scenario: This issue was observed in AP-220 Series connected to controllers running ArubaOS 6.3.1.1 or earlier.</p> |
| 91373 | <p>Symptom: MacBook clients were unable to pass traffic on the network. This issue was resolved by changes to ArubaOS that require APs to send data frames to all connected clients.</p> <p>Scenario: This issue was observed in AP-220 Series access points that were upgraded to ArubaOS 6.3.1.0, and was triggered by virtual APs being enabled or disabled, either manually (by network administrators) or automatically, as a part of the regular AP startup process.</p> |
| 91374 | <p>Symptom: Latency issues occur when clients are connected to a single AP.</p> <p>Scenario: This issue occurred on an AP-225 access point on a controller running ArubaOS 6.3.1 and later. This occurred when clients go into PS mode.</p> |

Table 96: AP-Wireless Fixed Issues

| Bug ID | Description |
|---|--|
| 91379 91449 91454 91480 94171 | <p>Symptom: An AP-220 Series device unexpectedly crashed. Using the correct structure to fill the information in the outgoing response frame resolved this issue.</p> <p>Scenario: The 802.11k enabled client that sent a Neighbor Report Request frame caused the AP-220 Series device to crash when the packet was freed. This issue was observed in controllers running ArubaOS 6.3.x or later.</p> <p>Duplicate Bugs: The following bug IDs have reported similar issues: 94238, 94413</p> |
| 91856 | <p>Symptom: Certain 802.11b clients did not communicate with 802.11n-capable access points. Improvements in the wireless driver of 802.11n-capable access points resolved this issue.</p> <p>Scenario: This issue was observed when Denso® 802.11b handy terminals communicated with 802.11n-capable access points on channel 7. This issue was not limited to a specific controller model or release version.</p> |
| 91770 91802 91805 91946 92052 | <p>Symptom: AP-135 stopped responding and rebooted. Improvements to the wireless driver in ArubaOS 6.1.3.2 resolved the issue.</p> <p>Scenario: This issue occurred when the buffer was corrupted in the wireless driver. This issue was observed in AP-135 running ArubaOS 6.3.1.0.</p> <p>Duplicate Bugs: The following bug IDs have reported similar issues: 92102, 92260, 92550, 92552, 92554, 92555, 92557, 92559, 92561, 92562, 92736, 92788, 92790, 92873, 92976, 92977, 93756, 93757, 93963</p> |
| 92346 | <p>Symptom: When the 80 MHz option is enabled in the RF arm-profile, HT Capabilities in beacon only show 20 MHz support.</p> <p>Scenario: This issue occurred on controllers with AP-225 access points running ArubaOS 6.3.1 and later.</p> |
| 92626 | <p>Symptom: An AP crashed and the log files for the event listed the reason for the crash as kernel panic. This issue is fixed by referencing the valid memory.</p> <p>Scenario: This issue occurred when an invalid memory was referenced. This issue occurred in AP-225 access points running ArubaOS 6.3.1.1.</p> |
| 92775 96408 | <p>Symptom: Wireless clients received Automatic Private IP Address (APIPA) when associated to AP-225. Improvements in the wireless driver of the AP fixed the issue.</p> <p>Scenario: This issue was seen when wireless clients associated to encryption-enabled tunnel-mode Virtual AP (VAP) on the AP-225 and there was one or more bridge or decrypt-tunnel VAPs configured with encryption mode set to static-wep.</p> |
| 93113 | <p>Symptom: Windows 7 clients using Intel 4965 NIC intermittently stopped passing traffic when connected to AP-225. Changes in the internal code resolved this issue.</p> <p>Scenario: This issue occurred on AP-225 running ArubaOS 6.3.1.1.</p> |
| 93288 | <p>Symptom: Some clients with low signal strength had trouble sending packets to an AP. Implementing the Cell-Size-Reduction feature on AP-220 Series along with deauthorizing clients when they are about to go out of the desired cell range resolved this issue.</p> <p>Scenario: This issue was observed in AP-220 Series connected to controllers running ArubaOS 6.3.1.1 or earlier.</p> |
| 93476 | <p>Symptom: Sporadic input/output control errors were seen in the logs of many APs. Changes in the internal code resolved this issue.</p> <p>Scenario: This issue was observed when the authentication manager tries to set the keys for previous association, then station sends deauthentication, or the AP disconnects the station.</p> |

Table 96: AP-Wireless Fixed Issues

| Bug ID | Description |
|---|--|
| 93710 94370 | <p>Symptom: Vocera clients associated to an AP were unable to communicate with the Vocera server. This issue was resolved by limiting the multicast transmission rate so that the unicast transmission is not affected.</p> <p>Scenario: This issue occurred when multicast traffic blocked hardware and software queues resulting in unicast packets being dropped. This issue is observed in AP-225 connected to controllers running ArubaOS 6.3.1.1.</p> |
| 93996 | <p>Symptom: An AP-120 Series access point rebooted unexpectedly. This issue is resolved by making changes to the internal code to avoid a potential condition that causes an infinite loop and NMI watchdog condition which causes the AP to reboot.</p> <p>Scenario: This issue occurred on AP-120 Series devices connected to controllers running ArubaOS 6.3.1.0.</p> |
| 94059 94520 95057 95106 95107 | <p>Symptom: An AP rebooted due to unhandled kernel unaligned access.</p> <p>Scenario: This issue was observed in AP-120 Series access points when the controllers were upgraded from ArubaOS 6.1.3.7 to 6.1.3.9, but is not limited to any specific controller model.</p> |
| 94117 | <p>Symptom: Clients are unable to connect to a SSID when the Local Probe Request Threshold setting in the SSID profile (which defines the SNR threshold below which incoming probe requests are ignored) is set to a value of 25 dB. This issue is resolved by changes that allow the AP to respond to probe requests with the same dB value as the local probe request threshold.</p> <p>Scenario: This issue was triggered in ArubaOS 6.3.1.x because when the Local Probe Request Threshold setting had a value of 25 dB in this setting, the AP did not respond to probe requests with SNR higher than 35 dB. As a result, APs did not respond to authentication requests from the clients, preventing them from associating to the AP.</p> |
| 94155 94249 | <p>Symptom: An AP-225 device rebooted unexpectedly when connected to a PoE. This issue is resolved by making code level changes in the index table.</p> <p>Scenario: This issue occurred due to the drastic peak in power when AP-225 is connected to 3af PoE (Power over Ethernet) and operates in low-power mode. This issue was observed in AP-225 connected to controllers running ArubaOS.</p> |
| 94164 94534 | <p>Symptom: Wireless clients were unable to connect to an AP through the G band when the WPA2 authentication scheme was used. This issue is resolved by changing the initial value of VHT (Very High Throughput) to 0.</p> <p>Scenario: This issue was observed in AP-225 connected to controllers running ArubaOS 6.3.1.1.</p> |
| 94198 | <p>Symptom: An AP rebooted unexpectedly with the log error message out of memory.</p> <p>Scenario: This issue occurred on the AP-120 Series running ArubaOS 6.3.1.0.</p> |
| 95006 | <p>Symptom: IOS devices faced connectivity issues after upgrading from 6.1.3.8 to 6.3.1.2. This issue is resolved by revising the received signal strength indication (RSSI) threshold value that triggers the handoff assist.</p> <p>Scenario: This issue was observed in controllers running ArubaOS 6.2 and 6.3 when the RSSI dropped below the defined threshold value.</p> |

ARM

Table 97: *ARM Fixed Issues*

| Bug ID | Description |
|--------|---|
| 93312 | Symptom: When location server was configured on the controller, a connected Air Monitor (AM) mode AP did not generate a probe report unless the location-feed flag was manually set through the AP console. Scenario: This issue occurred could occur on any model of AP operating in AM mode running ArubaOS 6.3.x.x. |

Authentication

Table 98: *Authentication Fixed Issues*

| Bug ID | Description |
|--------|--|
| 94629 | Symptom: The clients connected to RAPs lost connectivity when the process handling the AP management and user association crashed. This fix ensures that the AP management and user association process does not crash. Scenario: This issue was observed in controllers running ArubaOS 6.3 and 6.4. |
| 94964 | Symptom: Captive Portal users were forced to re-authenticate every 5-10 minutes as users were not sending the IPv6 traffic. This issue is resolved by making code level changes in the authentication module. Scenario: This issue was observed when wired users connected to an AP and IPv6 was enabled on the controller. This issue was limited only to release versions that supported IPv6 features. |

Base OS Security

Table 99: *Base OS Security Fixed Issues*

| Bug ID | Description |
|-------------------------|---|
| 86141 93351 93726 | Symptom: Issuing the show global-user-table list command displayed duplicate client information. Ignoring the master controller IP query in Local Management Switch (LMS) list fixed the issue. Scenario: This issue was observed in a VRRP or master-local deployment where the master controller queried itself and the LMS list resulted in duplicate client information. This issue was observed in controllers running ArubaOS 6.3.X.0. |
| 86867 | Symptom: When a user-role and the ACL that have the same name and were configured as the ip access-group on the interface for APs/RAPs, the AP/RAP traffic was hitting the user-role ACL instead of the ip access-group ACL. Scenario: This issue was observed on controllers running ArubaOS 6.2.1.2. |
| 87405 | Symptom: Firewall policies were not enforced on certain client traffic when the clients were connected to a RAP in wired mode and configured with a static IP. This issue is resolved by ensuring that the sessions established with untrusted users are deleted and recreated to apply the firewall policies correctly. Scenario: This issue was observed when the traffic was initiated by a device or server connected to the controller with an idle client. This issue was not limited to any specific controller model or release version. |

Table 99: Base OS Security Fixed Issues

| Bug ID | Description |
|----------------|--|
| 87742 | <p>Symptom: AP group information was not present in the RADIUS packet when the radio was disabled on the AP. The fix ensures that the AP group information is correctly populated in the RADIUS packet even when the radio is disabled.</p> <p>Scenario: This issue occurred when the wired clients were connected to the AP where BSSIDs were unavailable due to a disabled radio. This issue was not limited to any specific controller model or release version.</p> |
| 88271 | <p>Symptom: It was not possible to configure a deny any any protocol access control list (ACL) that overrode a statically configured permit any any protocol ACL. This issue is resolved by improvements that allow a user-defined ACL to take precedence over a static ACL entry.</p> <p>Scenario: This issue was observed on a controller running ArubaOS 6.3.0.1.</p> |
| 89453 | <p>Symptom: The show rights command did not display all the user roles configured in the controller. The output of this command now displays all the user roles configured in the controller.</p> <p>Scenario: This issue was observed when more than 50 user roles were configured on a controller running ArubaOS 6.2.1.3.</p> |
| 90180 | <p>Symptom: Re-authentication of the management users was not triggered upon password change. The users are now getting Password changed, please re-authenticate message on the console, forcing the user to login again with the new password.</p> <p>Scenario: The issue was observed when users were already connected, and the password for these users was changed. The re-authentication message for these users was not shown. This issue was not limited to any specific controller model or ArubaOS version.</p> |
| 90209 | <p>Symptom: A controller rebooted unexpectedly. The log files for the event listed the reason as datapath timeout.</p> <p>Scenario: The timeout occurred due to a VIA client sending an SSL fallback packet, where the third SSL record encapsulating the IPsec packet had an invalid IP header. This issue was not limited to a specific controller model and was observed in ArubaOS 6.2.1.2.</p> |
| 90233 | <p>Symptom: Clients with a logon user role did not age out from the user-table after the logonlifetime AAA timer expired. Users are mpw aged out with the logon user role if the User Derivation Rule (UDR) is configured in the AAA profile.</p> <p>Scenario: This issue was observed when UDR was configured in the AAA profile with the logon defined as the default user role. This issue was observed on controllers running ArubaOS 6.2.1.x.</p> |
| 90454 | <p>Symptom: A remote AP unexpectedly rebooted because it failed to receive heartbeat responses from the controller. Changes to the order in which new IPsec SAs are added and older IPsec SAs are removed resolved this issue.</p> <p>Scenario: This issue occurred after a random IPsec rekey, and was triggered when the outbound IPsec SA was deleted before the inbound IPsec SA was added. This removed the route cache for the inner IP, causing the session entry to incorrectly point to the default gateway, and preventing heartbeat responses from reaching the AP.</p> |
| 90904 92079 | <p>Symptom: In the ArubaOS Dashboard, under Clients > IP address, the IP addresses, Role Names, and names of clients connected to a RAP in split tunnel mode were not displayed.</p> <p>Scenario: The client information was not being sent correctly to through the controller and, therefore, not being displayed in the dashboard.</p> |
| 91548 | <p>Symptom: The error message User licensed count error appeared in the error log. However, the system functionality was not affected.</p> <p>Scenario: This issue occurred on controllers running ArubaOS 6.2.1.3 and later. This occurred when the VIA client connected to a RAP in split-tunnel or bridge-mode and the RAP was connected to the same controller from behind NAT.</p> |

Table 99: Base OS Security Fixed Issues

| Bug ID | Description |
|----------------|--|
| 92674 | <p>Symptom: Class attribute was missing in the Accounting STOP packet. This issue is resolved by not resetting the counters when an IPv6 user entry is deleted.</p> <p>Scenario: This issue occurred when the counters were reset during an IPv6 user entry aged out. This issue was not limited to any specific controller or ArubaOS version.</p> |
| 92817 | <p>Symptom: Wireless clients were blacklisted even when the rate of the IP Session did not exceed the threshold value set. This issue is resolved by increasing the storage of the threshold to 16 bits.</p> <p>Scenario: This issue was observed if the threshold of the IP Session rate was set to a value greater than 255. This issue was observed in controllers running ArubaOS 6.x.</p> |
| 93066 93868 | <p>Symptom: The MAPC module on the controller crashed unexpectedly. The log files for the event listed the reason for the crash as mapc segmentation fault. Internal code changes in the MAPC module of the controller fixed this issue.</p> <p>Scenario: This issue was observed when IF-MAP was configured on the controller to communicate with ClearPass Policy Manager (CPPM). This issue was observed on 7200 Series controllers running ArubaOS 6.3 or later versions.</p> |
| 93130 | <p>Symptom: A controller reboots unexpectedly. The log files for the event listed the reason for the reboot as datapath exception. This issue is resolved by adding SSL implementation to validate a packet before processing it.</p> <p>Scenario: This issue was observed when VIA was used to establish a tunnel with the controller, using SSL fallback. This issue was not limited to any specific controller model or ArubaOS version.</p> |
| 93237 | <p>Symptom: An internal module (Authentication) crashed on the controller. Ignoring the usage of the equivalentToMe attribute, which was not used by the master controller resolved this issue.</p> <p>Scenario: This issue was observed when the Novell Directory System (NDS) pushed the bulk of user data as the value for the attribute to the master controller. This issue was not limited to any specific controller model or ArubaOS version.</p> |
| 95367 | <p>Symptom: Issuing show rules <role-name> command from the command-line interface of a controller resulted in an internal module (Authentication) crash. Ensuring that Access Control Lists (ACLs) are not configured with spaces in the code resolved the issue.</p> <p>Scenario: This issue was observed when a large number of ACL was configured with spaces in their names. This was not limited to any specific controller model or ArubaOS version.</p> |

Configuration

Table 100: *Configuration Fixed Issues*

| Bug ID | Description |
|----------------------------------|--|
| 73459 85136 86427 90081 | Symptom: The output of the show acl hits CLI command and the Firewall Hits information on the UI Monitoring page of the controller WebUI showed inconsistent information. This issue is resolved by displaying consistent information. Scenario: This issue occurred because the formatting of the XML response from the controller to the WebUI was incorrect, when the output was beyond the specified limit. This issue was not limited to a specific controller model or release version. |
| 88120 | Symptom: The Configuration > Wireless > AP Installation > AP provisioning > Status tab of the controller WebUI and the output of the commands show ap database long status up start 0 sort-by status sort-direction ascending and show ap database long status up start 0 sort-by status sort-direction descending do not correctly sort the AP entries in ascending or descending order by up time. Improvements to how the controller sorts APs by status and up time resolve this issue. Scenario: This issue was identified in controllers running ArubaOS 6.2.1.2 |
| 91903 93462 93631 | Symptom: The controller's fpccli process crashed when executing the command show ap tech-support ap-name <ap name> with a non-existing or incorrect AP name. Now, when this command is executed with a non-existent AP, the CLI returns AP with name "X" not found. Scenario: This issue was observed on an M3 controller running ArubaOS 6.1.3.10 but was not limited to a specific controller model. |

Captive Portal

Table 101: *Captive Portal Fixed Issues*

| Bug ID | Description |
|-------------------------|---|
| 87294 87589 92575 | Symptom: Captive Portal (CP) whitelist that was mapped to the user-role did not get synchronized with the standby controller. Checks in the CP whitelist database fixed this issue. Scenario: This issue was observed when a net-destination was created and added to the CP profile whitelist that mapped to the user-role in the master controller. This issue was observed in ArubaOS 6.2.1.2 and was not limited to any specific controller model. |
| 88001 | Symptom: The domain name whitelist could not be configured using wild card characters in the Captive Portal profile. The fix ensures that the wild card characters are supported while configuring the domain name whitelist. Scenario: This issue was not limited to any specific controller model or release version. |
| 88116 | Symptom: Captive Portal user was incorrectly redirected to the User Authenticated page even when the user provided a wrong username or password. The user now gets an Invalid username or password error message when providing wrong credentials. Scenario: This issue was observed if MSCHAPv2 was used for Captive Portal authentication. This issue was not limited to a specific controller model or release version. |
| 88283 | Symptom: The captive portal profile used https by default. For authentication, the user was redirected to the https://securelogin.example.com. But if this URL was manually changed to http://securelogin.example.com, then connection remained insecure from that point onwards. The controller now sends a redirect URL using the protocol configured on the controller. Scenario: This issue was observed when there was a mismatch between the protocol configured on the AAA profile and the protocol from the browser, This issue was not limited to a specific controller model or release version. |

Table 101: *Captive Portal Fixed Issues*

| Bug ID | Description |
|--------|---|
| 88405 | <p>Symptom: After successfully authenticating a client using Captive Portal, the browser did not automatically redirect the client to the original URL.</p> <p>Scenario: This issue was observed in the 7200 Series controller running ArubaOS 6.3.0.0.</p> |
| 91442 | <p>Symptom: In the master controller's command line interface Login page, the question mark symbol was neither getting pushed nor getting added to the local controller. This issue is resolved by ensuring that the master controller's command line interface accepts the question mark symbol.</p> <p>Scenario: This issue was observed while synchronizing the configuration from the master controller to the local controller.</p> |
| 92170 | <p>Symptom: In Captive Portal, a custom welcome page did not redirect to the original Web page after successful client authentication. Changes in the Captive Portal code to send "url" cookie to the Web browser fixed this issue.</p> <p>Scenario: This issue was observed in controllers running ArubaOS 6.3.0.0 or later versions.</p> |
| 93674 | <p>Symptom: Clients were unable to access an external captive portal page after the controller reset. Changes in how ArubaOS manages captive portal authentication profiles resolved this issue.</p> <p>Scenario: This issue occurred in ArubaOS 6.1.3.x when the controller failed to use the correct ACL entry for a pre-authentication captive portal role.</p> |
| 94167 | <p>Symptom: When client traffic was moving through an L3 GRE tunnel between a switch and a controller, the controller did not provide the captive portal page to the client.</p> <p>Scenario: This issue was observed after an M3 was upgraded to ArubaOS 6.1.3.10. This issue was caused because the controller was unable to find the correct role for the client traffic and, therefore, did not provide the captive portal page.</p> |

Controller-Datapath

Table 102: *Controller-Datapath Fixed Issues*

| Bug ID | Description |
|---|--|
| 82770 | <p>Symptom: Using ADP, access points did not discover the master controller after enabling Broadcast/Multicast (BC/MC) rate optimization. With this new fix, enabling BC/MC rate optimization does not block ADP packets.</p> <p>Scenario: When BC/MC rate optimization was enabled on the VLAN, the controller dropped ADP packets from access points. This issue was not limited to a specific controller model or release version.</p> |
| 82824 | <p>Symptom: In some cases, when there was a large number of users on the network (more than 16k), and the Enforce DHCP parameter was enabled in the AP group's AAA profile, a user was flagged as an IP spoofed user. Changes to how ArubaOS manages route cache entries with the 'DHCP snooped' flag resolves this issue.</p> <p>Scenario: This issue was observed in controllers running ArubaOS 6.3.</p> |
| 83422 85600 87794 88311 88360 | <p>Symptom: A 7200 Series controller unexpectedly rebooted. The controller log files listed the reason for the event as a datapath timeout. Improvements in creating tunnels in the internal controller datapath resolved this issue.</p> <p>Scenario: This issue was observed in 7200 Series controllers running ArubaOS 6.2.1.x.</p> <p>Duplicate Bugs: The following bug IDs have reported similar issues: 88505, 88683, 88740, 88833, 88985, 89004, 89303, 89910, 90450, 90457, 90482, 90609, 90836, 91170, 91363, 91695, 92161, 92177, 92811, 93064, 93572, 93985, 94025, 94514</p> |

Table 102: Controller-Datapath Fixed Issues

| Bug ID | Description |
|---|--|
| 85398 85627 | <p>Symptom: A controller responded to the Domain Name System (DNS) queries even when the IP domain lookup was disabled. This issue is resolved by ensuring that the DNS service is completely stopped if the IP domain lookup is disabled.</p> <p>Scenario: This issue occurred when the controller responded to DNS requests with its own IP. This issue was observed in controllers running ArubaOS 6.1.3.6.</p> |
| 85685 85543 87406 | <p>Symptom: An M3 controller running ArubaOS 6.1.3.8 stopped responding and rebooted. The log files for the event listed the reason for the crash as fpapps: Segmentation fault. Changes to the process that handles the VLAN interfaces fixed the issue.</p> <p>Scenario: This issue was observed when the VLAN interface on the controller constantly switched between an UP and DOWN state, resulting in VRRP status change. This issue was not limited to a specific controller model or ArubaOS release version.</p> |
| 85796 88233 88731 90350 91310 | <p>Symptom: A controller crash was observed due to a session table entry corruption. This issue is resolved by modifying the method by which the IGMP query is handled over a port channel.</p> <p>Scenario: This issue occurred when an IGMP query was triggered on the port channel. This issue was observed in 3000 Series controllers, 7200 Series controllers, and M3 controllers running ArubaOS 6.2.x.</p> <p>Duplicate Bugs: The following bug IDs have reported similar issues: 93153, 93183</p> |
| 85843 | <p>Symptom: A controller unexpectedly rebooted. Log files for the event listed the reason for the reboot as datapath exception. Memory improvements resolve this issue in ArubaOS 6.4.</p> <p>Scenario: This issue was observed in a 7200 Series controller running ArubaOS 6.2.1.1.</p> |
| 87295 | <p>Symptom: A crash was observed in a controller when it received certain types of DNS packets. This issue is fixed by modifying the internal code to handle the DNS packets correctly.</p> <p>Scenario: This issue was observed when the firewall-visibility feature was enabled on a controller running ArubaOS 6.2 or later.</p> |
| 88325 | <p>Symptom: Enabling support for jumbo frames on an uplink interface caused pings larger than 1472 bytes to fail. This issue is resolved by changes that ensure ArubaOS uses the correct default MTU size when jumbo frames are disabled globally, while still enabled on a port.</p> <p>Scenario: This issue was observed in ArubaOS 6.3.1.0, on a controller with jumbo frames disabled globally, but enabled on a port.</p> |
| 88469 90779 | <p>Symptom: A controller denied any FTP download that used Extended Passive mode over IPv4. Modifying the FTP ALG to handle Extended Passive mode correctly resolved this issue.</p> <p>Scenario: This issue was observed when an IPv4 FTP client used Extended Passive mode. In such a case, the FTP ALG on the controller detected it as a Bounce Attack and denied the session. This issue was not limited to a specific controller model or release version.</p> |
| 87417 87846 87949 88039 88226 | <p>Symptom: A master controller rebooted unexpectedly. The log files for the event listed the reason for the reboot as datapath exception. Enhancements to the Broadcom driver of the access point fixed this issue.</p> <p>Scenario: This issue was observed in 7240 controller running ArubaOS 6.3.1.1 in a master-local topology.</p> <p>Duplicate Bugs: The following bug IDs have reported similar issues: 88445, 89433, 89539, 89641, 90024, 90458, 90469, 90746, 90896, 91853, 92284, 92464, 92466, 92827, 92828, 92829, 92830, 92832, 94007, 95012</p> |

Table 102: *Controller-Datapath Fixed Issues*

| Bug ID | Description |
|---|--|
| 87949 88039 88226 88445 89433 | <p>Symptom: A controller stopped responding to network traffic and rebooted. The log file for the event listed the reason for the reboot as datapath timeout. This fix ensures that the CPU livelock does not recur.</p> <p>Scenario: This issue occurred on 7200 Series controllers running ArubaOS 6.3.0.1 and 6.2.x.x.</p> <p>Duplicate Bugs: The following bug IDs have reported similar issues: 89539, 89641, 90024, 90458, 90469, 90746, 90896, 91853, 92294, 92464, 92466, 92827, 92828, 92829, 92830, 92832, 92988, 93555</p> |
| 89906 92248 93423 94010 94682 | <p>Symptom: A controller unexpectedly rebooted and the log file listed the reason for the reboot as datapath timeout. This issue is fixed by increasing the stack memory size in the data plane.</p> <p>Scenario: This issue was observed when clients using SSL VPN connected to RAP and the controller tried to decompress these packets. This issue is not limited to any specific controller model or ArubaOS release version.</p> <p>Duplicate Bugs: The following bug IDs have reported similar issues: 94989, 95215, 95958</p> |
| 93874 | <p>Symptom: With Multiple TID Traffic to Temptrak device with AES Encryption, the device drops packets from AP.</p> <p>Scenario: This issue was observed on ArubaOS 6.3.1.1 and is specific to 7200 Series controllers. This issue occurred because the controller was using multiple replay counters, which the device did not support.</p> |
| 93466 | <p>Symptom: The 7200 Series controllers rebooted and the log files for the event displayed the reason for the reboot as datapath timeout. This issue is fixed by not forwarding the mirrored packets to monitor port when the monitor port status is down.</p> <p>Scenario: This issue was observed when the port monitor was enabled on the controller and then a Small Form-factor Pluggable (SFP) was plugged in the monitor port. This issue was observed in 7200 Series controllers and was not limited to a specific ArubaOS version.</p> |
| 95927 | <p>Symptom: Winphone devices were unable to pass traffic as the ARP requests from the devices were considered as ARP spoofs . This issue is resolved by using DHCP binding to verify if the IP address acquired by the device was already used by an old user in the controller and avoid incorrect determination of a valid ARP request as spoof.</p> <p>Scenario: This issue was observed when the devices acquired an IP address that was used by an old user earlier on the controller. This issue is not limited to any specific controller model or release version.</p> |
| 95588 | <p>Symptom: GRE tunnel groups sessions initiated by remote clients failed. This issue is resolved by redirecting the traffic initiated only by local clients.</p> <p>Scenario: This issue was observed when traffic from remote clients was redirected. This issue was observed in controllers running ArubaOS 6.3 or later.</p> |

Controller-Platform

Table 103: *Controller-Platform Fixed Issues*

| Bug ID | Description |
|---|--|
| 70068 85684 87008 | <p>Symptom: An internal controller module stops responding when a user attempts to add or delete a large number of VRRP instances. This issue is resolved by internal work flow enhancements that prevent this issue from occurring.</p> <p>Scenario: This error can be triggered by a VRRP state change, enabling or disabling an interface, or adding or deleting a tunnel.</p> |
| 82402 84212 86636 87552 89437 | <p>Symptom: A controller unexpectedly stopped responding and rebooted. The log files for the event listed the reason for the crash as httpd_wrap process died. Verifying the Process Application Programming Interface (PAPI) packet before processing it resolved the issue.</p> <p>Scenario: This issue was observed when the PAPI library used by all applications did not filter the broadcast traffic correctly prior to PAPI inspection that caused the applications to crash. This issue occurred in 3400 controllers running ArubaOS 6.2.1.0.</p> <p>Duplicate Bugs: The following bug IDs have reported similar issues: 90466, 91280, 93591, 94721, 94727, 95074, 95624, 95643, 95644</p> |
| 82736 82875 83329 83762 84022 | <p>Symptom: A controller rebooted unexpectedly. Changes in the watchdog implementation on the controller resolved the issue.</p> <p>Scenario: Log files for the event indicated the reasons for the reboot were soft watchdog reset or user pushed reset. This issue was identified in ArubaOS 6.1.x.x, and is not limited to any specific controller model.</p> <p>Duplicate Bugs: The following bug IDs have reported similar issues: 85355, 85370, 85628, 86005, 86029, 86031, 86572, 86589, 87410, 87505, 87587, 88005, 88332, 88351, 88434, 88921, 89636, 89818, 90909, 91269, 91308, 91370, 91517, 92823, 93294, 93770, 95946</p> |
| 83502 83762 85355 85370 86029 | <p>Symptom: A controller rebooted unexpectedly. Changes in the watchdog implementation on the controller resolved the issue.</p> <p>Scenario: Log files for the event indicated the reason for the reboot as user pushed reset. This issue was identified in ArubaOS 6.1.3.x, and is not limited to a specific controller model.</p> <p>Duplicate Bugs: The following bug IDs have reported similar issues: 86031, 88005, 89636, 92823</p> |
| 85685 92814 | <p>Symptom: An M3 controller stopped responding and rebooted due to an internal memory leak. Internal code changes fixed the memory leak.</p> <p>Scenario: This issue occurred after the show running-config or write memory command was executed on the controller on which the static or default routes were not configured. This issue was observed in M3 controllers running ArubaOS version 6.2.1.3 or later.</p> |
| 86107 93279 | <p>Symptom: The controller stopped processing radius packets every three hours and then resumed after one minute. This issue was resolved by setting aaa profile <aaa-profile-name> to no devtype-classification for all aaa profiles in use. Then execute the clear aaa device-id-cache all command.</p> <p>Scenario: An internal process took a backup of the database every three hours, and during this time authentication tried to access information from the database and waited there until backup was complete. Authentication resumed after that. This issue was observed on controllers running ArubaOS 6.2 or earlier.</p> |
| 86216 85566 87090 87635 88321 | <p>Symptom: During a kernel panic or crash, the panic dump generated by the controller was empty. New infrastructure has been added to improve the collection of crash dumps.</p> <p>Scenario: This issue impacts 3000 Series, 600 Series, and M3 controllers and was observed on ArubaOS 6.1.3.7.</p> <p>Duplicate Bugs: The following bug IDs have reported similar issues: 88387, 88699, 89436, 89727, 89839, 89911, 90162, 90338, 90481, 91193, 91387, 91941, 92139, 92187, 92516, 92808,,93630, 93693, 93931, 94308</p> |

Table 103: *Controller-Platform Fixed Issues*

| Bug ID | Description |
|---|--|
| 86266 | <p>Symptom: In rare cases, issuing commands through a telnet shell caused an internal controller process to stop responding, triggering an unexpected controller reboot. This issue is resolved by changes that prevent ArubaOS from referencing null pointers within the software.</p> <p>Scenario: This issue was triggered by varying sequences of commands issued via the telnet shell, and is not specific to a controller model or release version.</p> |
| 87498 | <p>Symptom: An internal process (FPAPPS) failed unexpectedly.</p> <p>Scenario: This issue occurred on a 3200 controller running ArubaOS 6.3.0.1 when the PPOE/PPP connection was established.</p> |
| 89155 | <p>Symptom: 600 Series controllers experienced high levels of CPU usage while booting, triggering the warning messages Resource 'Controlpath CPU' has exceeded 30% threshold. This issue is resolved by changes to internal CPU thresholds that better reflect expected CPU usage levels.</p> <p>Scenario: This issue was observed in controllers running ArubaOS 6.1.2.3.</p> |
| 90751 90633 90863 91154 91138 | <p>Symptom: Controllers continuously stopped responding and rebooted. Enhancements to memory allocation resolved this issue.</p> <p>Scenario: The issue occurred when an internal module (FPCLI) crashed due to memory corruption. This issue was observed in M3 controllers and is not limited to a specific ArubaOS version.</p> <p>Duplicate Bugs: The following bug IDs have reported similar issues: 91474, 91656</p> |
| 90619 92250 | <p>Symptom: The controller WebUI stopped responding indefinitely. The fix ensures that the AirWave query fails if there is no firewall visibility.</p> <p>Scenario: This issue occurred when AirWave queried for firewall visibility details from a controller on which the firewall visibility feature was disabled. This issue was observed in controllers running ArubaOS 6.2 or later.</p> |
| 91383 | <p>Symptom: Executing a show command causes the controller command-line interface to display an error: Module Configuration Manager is busy. Please try later. Improvements to how the controller manages HTTP session keys resolved this issue.</p> <p>Scenario: This issue occurred when issuing show commands from the command-line interface of a 3000 Series standby controller, and is triggered when the database synchronization process attempts to simultaneously replace and add an HTTP session key in the user database.</p> |
| 91778 | <p>Symptom: A controller unexpectedly reboots, displaying the error message Mobility Processor update.</p> <p>Scenario: This issue was observed in a local M3 controller module running ArubaOS 6.3.x.x in a master-local topology.</p> |
| 93990 | <p>Symptom: A few Not Found error messages appeared in the controller's console while performing initial configuration while booting. Modifying the make subsystem, and packaging the binary resolved this issue. Scenario: A certain binary was not built correctly due to changes in make or packaging script. This issue was observed in 600 Series controllers running ArubaOS 6.1.x.x or later.</p> |
| 94013 94045 95079 | <p>Symptom: A controller rebooted due to low memory. Changes in the internal code of the controller software fixed this issue.</p> <p>Scenario: This issue occurred when there was continuous high traffic terminating on the control plane. This resulted in an internal component of the ArubaOS software to take up high memory. This issue was observed in 600 Series, 3000 Series, and M3 controllers running ArubaOS 6.1 or later versions.</p> |
| 95044 | <p>Symptom: All access points went down when the controller to which they were connected rebooted and an error was displayed - Ancillary image stored on flash is not for this release. This issue is resolved by writing the boot partition information to the secondary bank of the NVRAM.</p> <p>Scenario: This issue occurred when the controller rebooted due to a watchdog reset. This issue is observed only in 7200 Series controllers.</p> |

Control Plane Security

Table 104: *Control Plane Security Fixed Issues*

| Bug ID | Description |
|--------|--|
| 85402 | Symptom: When sending the RAP whitelist information to CPPM, ArubaOS did not fill the Calling-Station-Id correctly. Scenario: The controller returned a Calling-Station-Id value of 000000000000 instead of the actual value. This issue was caused by a malfunction in an internal controller process (auth) and was observed on a controller running ArubaOS 6.3.0. |

DHCP

Table 105: *DHCP Fixed Issues*

| Bug ID | Description |
|--------|--|
| 90611 | Symptom: The Dynamic Host Configuration Protocol (DHCP) module crashed on a controller and users were not able to perform a new DHCP configuration. The updates to the DHCP wrapper fixed this issue in ArubaOS 6.4. Scenario: This issue was triggered by a race condition that caused the DHCP wrapper process to crash with continuous restarts. This issue was not limited to a specific controller model or release version. |
| 92438 | Symptom: Dynamic Host Configuration Protocol (DHCP) logs were displayed even when the DHCP debug logs were not configured. The fix ensures that the DHCP logs are printed only when the debug log is configured. This issue is resolved by changing the DHCP debug log configuration. Scenario: This issue was observed on controllers running ArubaOS 6.2 or later. |

Generic Routing Encapsulation

Table 106: *Generic Routing Encapsulation Fixed Issues*

| Bug ID | Description |
|--------|--|
| 89832 | Symptom: Layer 2 Generic Routing Encapsulation (L2 GRE) tunnel between L2 connected controllers dropped because of keepalive failures. This issue is fixed by bridging the packets before routing in the forwarding pipeline. Scenario: This issue occurred when the GRE tunnel keep alive was enabled and the Configuration > Network > IP > IP Interface > Edit VLAN (1) > Enable Inter-VLAN Routing option was disabled. This issue was observed in controllers running ArubaOS 6.3 configured with L2 GRE tunnel between L2 connected switches. |

GSM

Table 107: *GSM Fixed Issues*

| Bug ID | Description |
|--------|---|
| 91870 | Symptom: The output of the show ap database command indicated that a RAP-5 was inactive and that the RAP-5 would not come up. This issue is resolved by increasing the allocation for AP wired ports to 16x. Scenario: This issue was observed with RAP-5 APs when all four wired AP ports were enabled in ArubaOS 6.3. ArubaOS 6.3 introduced GSM where space was pre-allocated for the AP wired ports based on the maximum number of APs times the maximum number of wired ports, because RAP-5 has four wired ports and the controller allowed four times the campus APs. As a result, the number of GSM slots was insufficient. |

Guest Provisioning

Table 108: *Guest Provisioning Fixed Issues*

| Bug ID | Description |
|--------|---|
| 87091 | <p>Symptom: The Guest Provisioning page of the WebUI showed incorrect alignment when it was printed from the Internet Explorer 8 or the Internet Explorer 9 Web browser. Improvements in the HTML styles resolved this issue.</p> <p>Scenario: This issue was first identified in ArubaOS 5.0.4.0. This issue was not observed when users viewed the controller WebUI using older versions of Internet Explorer (version 6 and 7).</p> |

HA-Lite

Table 109: *HA-Lite Fixed Issues*

| Bug ID | Description |
|--------|---|
| 80206 | <p>Symptom: The high availability: fast failover feature introduced in ArubaOS 6.3 did not support VRRP-based LMS redundancy in a deployment with master-master redundancy. This topology is supported in ArubaOS 6.4.</p> <p>Scenario: This issue occurred because the high availability: fast failover feature does not allow the APs to form standby tunnels to the standby master controller.</p> |

Hardware Management

Table 110: *Hardware Management Fixed Issues*

| Bug ID | Description |
|--------|--|
| 87481 | <p>Symptom: 7200 Series controller returned an invalid value when an SNMP query was performed on the internal temperature details (OID .1.3.6.1.4.1.14823.2.2.1.2.1.10). The fix ensures that the SNMP attribute is set correctly for the temperature details.</p> <p>Scenario: This issue was limited to 7200 Series controllers running ArubaOS 6.3 or later versions.</p> |

IGMP Snooping

Table 111: *IGMP Snooping Fixed Issues*

| Bug ID | Description |
|--------|--|
| 93737 | <p>Symptom: The ERROR: IGMP configuration failed error message was displayed when the IGMP proxy was configured using the WebUI. This issue is resolved by ensuring that only one of the following radio buttons - Enable IGMP, Snooping, or Proxy under the Configuration > Network > IP > IP Interface > Edit VLAN page of the WebUI is enabled.</p> <p>Scenario: This issue was not limited to any specific controller model or ArubaOS version.</p> |

IPv6

Table 112: *IPv6 Fixed Issues*

| Bug ID | Description |
|--------|--|
| 88814 | <p>Symptom: When clients connected to a controller, they received IPV6 router advertisements from VLANs with which they were not associated. This issue is resolved by updating the datapath with the router advertisements conversion flag, so that datapath converts multicast router advertisements to unicast.</p> <p>Scenario: This issue was observed in IPv6 networks with derived VLANs and was not limited to a specific controller model or release version.</p> |

Licensing

Table 113: *Licensing Fixed Issues*

| Bug ID | Description |
|--------|--|
| 87424 | <p>Symptom: The licenses were lost on a standby master controller due to which the configuration on the local controller was also lost. Caching the master controller's license limits on the standby controller for a maximum of 30 days resolved this issue.</p> <p>Scenario: This issue occurred when the standby comes up before the master after a reboot. This occurred in all master scenarios when running ArubaOS 6.3 or later.</p> |
| 89294 | <p>Symptom: RAPs were unable to come up on a standby controller if the AP licenses were installed only on the master controller.</p> <p>Scenario: This issue occurred when centralized licensing was enabled and all AP licenses were installed on the master controller and the RAP feature was disabled on the standby controller. This issue was observed in controllers running ArubaOS 6.3.</p> |

Local Database

Table 114: *Local Database Fixed Issues*

| Bug ID | Description |
|--------|---|
| 88019 | <p>Symptom: A warning message WARNING: This controller has RAP whitelist data stored in pre-6.3 format, which is consuming running the command 'local-userdb-ap del all appeared when a user logged into the controller. This issue is fixed by deleting the warning file when all the old entries are deleted.</p> <p>Scenario: This issue occurred when a controller was upgraded from a previous version of ArubaOS to 6.3 or later version. This issue was not limited to any specific controller model or release version.</p> |

Master-Redundancy

Table 115: *Master-Redundancy Fixed Issues*

| Bug ID | Description |
|----------------------------------|--|
| 80041 87032 87946 88067 | <p>Symptom: The show database synchronize command displayed a FAILED message and the standby controller was out of sync with the Master. Additionally, if there is a switchover at this time, the system is in an inconsistent state. This issue is resolved by ignoring any aborted database's synchronization sequence number on the master controller, so that the subsequent database synchronization can proceed without waiting for a response from the standby controller for previous aborted database synchronization.</p> <p>Scenario: This issue occurred when a controller was upgraded from a previous version of ArubaOS to 6.3 or later version. This issue was not limited to any specific controller model or release version.</p> |

Mesh

Table 116: *Mesh Fixed Issues*

| Bug ID | Description |
|-------------------------|--|
| 89458 91343 92614 | <p>Symptom: A Mesh Point rebooted frequently as it could not connect to a Mesh Portal. This issue is resolved by allowing Mesh Point to use the configured power for transmitting probe requests instead of reduced power.</p> <p>Scenario: This issue occurred when the transmission power on the Mesh Point was very low compared to the configured power. This issue was observed in AP-105 and AP-175 with controllers running ArubaOS 6.1.x and later versions.</p> |

Mobility

Table 117: *Mobility Fixed Issues*

| Bug ID | Description |
|--------|--|
| 88281 | <p>Symptom: IP mobility entries were not cleared even when the client leaves the controller and user entries aged out. Additionally, the command clear ip mobile host <mac-address> did not clear the stale entry.</p> <p>Scenario: This issue was caused by a message loss between the controller's Mobile IP and authentication internal processes. Due to the message loss, the affected clients were blocked. This issue was observed in controllers running ArubaOS 6.3.x, 6.2.x, and 6.1.x.</p> |

PPPoE

Table 118: *PPPoE Fixed Issues*

| Bug ID | Description |
|--------|--|
| 86681 | <p>Symptom: A controller was not able to connect to the Internet. This issue is fixed by modifying the way Point-to-Point Protocol over Ethernet (PPPoE) handles user name that contains special characters.</p> <p>Scenario: The PPPoE connection was not established with an internet service provider (ISP) server when a PPPoE user name contained special characters (for example: #0001@t-online.de). This issue was observed on controllers running ArubaOS 6.1.3.7 or later.</p> |
| 94356 | <p>Symptom: PPPoE connection did not work with 'ip nat inside' configuration. Changes to the logic that prevented NAT to occur in datapath fixed this issue.</p> <p>Scenario: This issue was observed on controllers with uplink as a PPPoE interface, and the client VLAN has 'ip nat inside' enabled.</p> |

Remote AP

Table 119: *Remote AP Fixed Issues*

| Bug ID | Description |
|--------|---|
| 82015 | <p>Symptom: An AP associated with a controller did not age out as expected when you changed the heartbeat threshold and interval parameters. Changes in the internal code fixed this issue.</p> <p>Scenario: This issue occurred when you changed the heartbeat threshold and interval parameters in the AP's system profile while the AP's status is UP in the controller. This issue was not limited to any specific controller, AP model, or ArubaOS release version.</p> |
| 85249 | <p>Symptom: A degradation of Transmission Control Protocol (TCP) throughput by 9 to 11 Mbps was observed on a RAP. This issue is resolved by optimizing driver code.</p> <p>Scenario: This issue occurred in RAPs with any forwarding mode and not specific to any AP model.</p> |
| 85970 | <p>Symptom: RAPs were rebooting or crashing with a reboot reason as Kernel page fault at virtual address. This issue is resolved by adding a check while processing packets with no session entry.</p> <p>Scenario: This issue was observed when the RAPs received some packets with no session entries from the IPsec tunnel. This issue was observed only in RAPs running ArubaOS 6.2.x.</p> |
| 86650 | <p>Symptom: A controller sent continuous RADIUS requests for the clients connected behind the wired port of a remote AP (RAP). This issue is resolved by ArubaOS enhancements that prevent memory corruption. Scenario: This issue was observed when a RAP used a PPPoE uplink and operated as a wired AP in split-tunnel or bridge mode. This issue occurred on ArubaOS running 6.1.3.6, and was not limited to any specific controller model.</p> |
| 86934 | <p>Symptom: The AP failed during boot up when the Huawei® modem E1371 was used. Clearing an empty device descriptor of the modem fixed the issue.</p> <p>Scenario: This issue was caused by an internal code error when using this modem. This issue was observed in RAP-108 and RAP-109 running ArubaOS 6.3.</p> |
| 88193 | <p>Symptom: BOSE WiFi products were not able to acquire an IP address through the internal built-in DHCP server in a RAP-5WN.</p> <p>Scenario: This issue occurred on controllers running ArubaOS 6.1.3.9 and later. The DHCP client did not receive an DHCP offer or acknowledgment from the DHCP server.</p> |
| 90355 | <p>Symptom: AP-70 and RAP-108 access points connecting to the network using a cellular uplink were not able to achieve a 3G connection. This issue is resolved by improvements to the AP boot process, and changes that allow cellular modems to support multiple ports on the AP.</p> <p>Scenario: This issue was observed in 6.3.x.x and 6.2.x.x, when AP-70 and RAP-108 access points connected to a Huawei® E220 Modem.</p> |
| 91106 | <p>Symptom: When a Remote Access Point (RAP) was rebooted from the controller using the apboot command, the system did not generate a log message. Changes to the internal code for handling log messages fix this issue.</p> <p>Scenario: This issue was observed in Remote Access Points running ArubaOS 6.1.x.x.</p> |
| 91292 | <p>Symptom: A Remote AP (RAP) failed over from backup LMS to primary and did not shutdown wired port. This issue is fixed by ensuring that the wired port is shut down initially when a failover occurs from backup LMS to primary LMS and then reconnects to primary LMS. This ensures that the wired port is enabled and the DHCP process is initiated.</p> <p>Scenario: This issue occurred when wired clients retained the old IP address retrieved from backup LMS and connected to primary LMS with LMS pre-emption enabled. This issue was observed in RAPs running ArubaOS 6.3.1.0.</p> |

Table 119: *Remote AP Fixed Issues*

| Bug ID | Description |
|--------|---|
| 93707 | <p>Symptom: The RAP reboots every 6 minutes if the RAP's local gateway IP is 192.168.11.1.</p> <p>Scenario: This issue occurred on controllers running ArubaOS 6.2.1.4 and 6.3.1.1. It was caused by the DHCP server net assignment conflicting with the RAP's local networks.</p> |
| 94140 | <p>Symptom: IAP whitelist database on the controller did not allow multiple APs in same branch to share a common remote IP.</p> <p>Scenario: Starting with ArubaOS 6.4, this option is now supported. This issue was caused by a typecasting error that prevented smaller IP addresses from being allowed.</p> |
| 94703 | <p>Symptom: IAP-VPN connection disconnected intermittently. This issue is resolved by not allowing IAP database to store more than six subnets per branch.</p> <p>Scenario: This issue was observed when IAP database had more than six subnets-per-branch although a maximum of six subnets-per-branch is allowed. IAP-VPN branch with six subnets went down for more than idle timeout and came up with different DHCP profiles which led to more than six subnet entries for the branch in the IAP database.</p> |

Role/VLAN Derivation

Table 120: *Role/VLAN Derivation Fixed Issues*

| Bug ID | Description |
|--------|---|
| 88508 | <p>Symptom: User derived roles were not considered for DHCP options. This issue is resolved by removing the ceiling limit set on the packet length.</p> <p>Scenario: This issue was observed when the DHCP packet length was greater than 1000 bytes in controllers running ArubaOS versions 6.3.x or earlier versions.</p> |

SNMP

Table 121: *SNMP Fixed Issues*

| Bug ID | Description |
|-------------------------|--|
| 85119 | <p>Symptom: The wlsxNLowMemory trap could not be triggered when the free memory of a controller was low. This issue is fixed by allowing a controller to send the wlsxNLowMemory trap, when the free memory of a controller reaches a threshold of 50 Mb. When the free memory of a controller reaches more than 50 Mb, the controller sends the wlsxMemoryUsageOK trap.</p> <p>Scenario: This issue occurred because the wlsxNLowMemory trap was not implemented. This issue was observed in controllers running ArubaOS 6.x.</p> |
| 83948 85146 87842 | <p>Symptom: The Simple Network Management Protocol (SNMP) module crashed when the management interface was deactivated while an SNMP query was running. A build option was modified to avoid generating code that may access invalid memory.</p> <p>Scenario: This issue was observed when SNMP was enabled and AirWave was used to monitor 620 and 3600 controllers running ArubaOS 6.3.0.0.</p> |
| 90453 | <p>Symptom: The wlsxStackTopologyChangeTrap SNMP trap was seen on AirWave from the controller AirWave doesn't support. This issue is resolved by updating to the latest ArubaOS MIBs on AirWave.</p> <p>Scenario: This issue was observed on controllers running AirWave 7.7.4 and ArubaOS 6.3.0.1.</p> |
| 94205 | <p>Symptom: The sysExtFanStatus MIB could not be queried. This issue is resolved by initializing the value of the fanCount.</p> <p>Scenario: This issue was triggered when the hwMon process did not return the proper value for fanStatus SNMP queries. This issue occurred in 7200 Series controllers running ArubaOS 6.3.1.1.</p> |

Station Management

Table 122: *Station Management Fixed Issues*

| Bug ID | Description |
|---|---|
| 85662 84880 88009 88319 89321 | Symptom: The state of APs were displayed as down on the master controller even if these APs were connected and UP. Internal code changes resolved this issue. Scenario: This issue was observed when AP's system profile had a local controller as the primary Local Management Switch (Primary-LMS) and master controller was configured as a backup Local Management Switch (Backup-LMS). This issue was not limited to any specific controller model and occurred in ArubaOS 6.3 or later. Duplicate Bugs: The following bug IDs have reported similar issues: 91963, 92164, 93243, 93388, 93389, 93984 |
| 86357 | Symptom: Station Down messages were not logged in the syslog messages. Changes to syslog messaging resolved this issue. Scenario: This issue was observed in controllers running ArubaOS 6.3.x.x. |
| 88938 88999 | Symptom: A controller's internal station management module stopped responding, causing the AP-125 access points associated to that controller to rebootstrap. Improvements to the process that updates internal tables for the client match feature resolve this issue. Scenario: This issue occurred on controllers running ArubaOS 6.3.0.1 and using the client match feature. |

TACACS

Table 123: *TACACS Fixed Issues*

| Bug ID | Description |
|--------|--|
| 89676 | Symptom: Users were not able to authenticate against a TACACS server. Scenario: This issue was observed in controllers running ArubaOS 6.1.3.7 and later. This was triggered when non-blocking sockets for TCP connect() were not polled long enough (at least 2-3 seconds are required) before closing the tcp socket. |

VLAN

Table 124: *VLAN Fixed Issues*

| Bug ID | Description |
|--------|--|
| 95622 | Symptom: The even VLAN distribution did not work correctly as the VLAN assignment number and the AP VLAN usage number did not match. The fix ensures that the VLAN assignment and AP VLAN usage numbers match. Scenario: This issue was observed in clients that were frequently roaming when even VLAN distribution was enabled. This issue was observed in controllers running ArubaOS 6.3.1.2. |

Voice

Table 125: *Voice Fixed Issues*

| Bug ID | Description |
|-------------------------|--|
| 77716 88996 90000 | <p>Symptom: Incompatibility issues observed between a 3600 controller and a Cisco CUCM using SCCP version 20. Users were able to make and receive calls using a Cisco phone but there was no audio. This issue is resolved by changes that allow the controller to handle Open Receive Channel Acknowledge (ORCA) messages for SCCP Version 20.</p> <p>Scenario: The Cisco CUCM was compatible with the Skinny Client Control Protocol (SCCP) version 20, while the 3600 controller supported only up to version 17 of the SCCP. This incompatibility issue resulted in media traffic not passing through the 3600 controller as the controller was not able to parse the SCCP signaling packets. This issue was observed in a 3600 controller running ArubaOS 6.0 or later.</p> |
| 86224 | <p>Symptom: Calls dropped after 30 seconds when performing a blindly transferred SIP call. Ignoring the mid call re-invite message (by SIP ALG state machine) handling process resolves the issue.</p> <p>Scenario: This issue was observed on the M3 controller module running ArubaOS version 6.2.1. It occurred when Ascom phones sent a DELTS request upon receiving either an "invite" message from the SIP server or after sending a "180 Ringing" message back to the server.</p> |
| 86683 | <p>Symptom: The show voice call-cdrs and show voice client-status command outputs did not display the call details for Lync wired clients with media classification configured on session ACL. This issue is resolved by ensuring to handle the message appropriately for wired clients.</p> <p>Scenario: This issue was observed when Lync clients were identified as voice clients via media classification. This issue occurred on ArubaOS running 6.2 and 6.3 versions, and not limited to any specific controller version.</p> |
| 93517 | <p>Symptom: Access point rebooted unexpectedly resulting in wireless clients losing network connectivity. Releasing CDR events for AP statistics and AP event in the CDR buffer resolved the issue.</p> <p>Scenario: This issue was observed in a VoIP deployment when the Station Management (STM) process that handles AP management and user association crashed on the controller. This issue was observed in controllers running ArubaOS 6.1 or later versions.</p> |

WebUI

Table 126: *WebUI Fixed Issues*

| Bug ID | Description |
|----------------|--|
| 73459 | <p>Symptom: The output of the show acl hits command and the firewall hits information on the Monitoring page of the controller WebUI shows inconsistent information. The issue is resolved by displaying consistent information in the CLI and WebUI.</p> <p>Scenario: This issue occurred because the formatting of the XML response from the controller to the WebUI was incorrect, when the output exceeded the specified limit. This issue was not limited to a specific controller model or release version.</p> |
| 76439 | <p>Symptom: The Spectrum Analysis section of the WebUI fails to respond when a connected spectrum monitor is in a DOWN state. Changes to how ArubaOS manages popup error messages resolve this issue.</p> <p>Scenario: This issue occurred in ArubaOS 6.2.0.0, when an AP-105 access point in hybrid AP mode failed to appear as a connected spectrum monitor in the controller WebUI.</p> |
| 85225 | <p>Symptom: The following two issues were observed when adding an SNMPv3 user under the Configuration > Management > SNMP page of the WebUI:</p> <ol style="list-style-type: none"> 1. User Name field was not editable. 2. Privacy Protocol value changed to null, when the Authentication Protocol was edited in SNMPv3 user entry. <p>The first issue is an expected behavior for SNMPV3 users and the button caption is changed to DONE in the Edit mode. The second issue is fixed by avoiding the Privacy Protocol value changing to null.</p> <p>Scenario: This issue was not limited to any specific controller model or release version.</p> |
| 87457 | <p>Symptom: The PKCS#12 Passphrase field was incorrectly enabled while provisioning a regular remote AP in the WebUI (under the Configuration > Wireless > AP Installation > Provision page). The PKCS#12 Passphrase field is now enabled in the WebUI only for provisioning a certificate based remote AP.</p> <p>Scenario: This issue was not limited to a specific controller model or software version.</p> |
| 87078 | <p>Symptom: While accessing AP Configuration or Authentication options, the system displayed show aaa authentication mgmt: data null error. This issue is resolved by restarting an internal process in the controller.</p> <p>Scenario: This issue was observed in 3200 Series controllers running ArubaOS 6.1.3.5.</p> |
| 87720 | <p>Symptom: The Reset button on the Monitoring page was not functioning correctly. The Reset button now resets all Air Monitors correctly.</p> <p>Scenario: This issue was not limited to a specific controller model or release version.</p> |
| 88066 | <p>Symptom: Users were unable to generate Certificate Signing Request (CSR) with a comma in the Organization field in the WebUI and displayed a message Invalid Character(s) Input for Organization. This issue is fixed by GUI updates to allow comma in the Organization field.</p> <p>Scenario: This issue occurred only in the WebUI and there was no impact in the Command Line Interface (CLI). This issue was not limited to any specific controller model or release version.</p> |
| 88398 | <p>Symptom: Network administrators were unable to manually contain or reclassify a group of detected rogue APs in the Dashboard > Security page of the WebUI. This issue is fixed by adding support to select multiple rogue APs .</p> <p>Scenario: This issue occurred when multiple rogue APs were selected in the Dashboard > Security page. This issue was observed in controllers running ArubaOS 6.2.1.3.</p> |
| 88802 91141 | <p>Symptom: When the client tried to access the Air Group option from the WebUI, the system did not respond. To resolve this issue the Air Group option is now removed from the WebUI for 600 Series controllers.</p> <p>Scenario: This issue was observed only in 600 Series controllers running ArubaOS 6.3.x.</p> |

Table 126: *WebUI Fixed Issues*

| Bug ID | Description |
|----------------|--|
| 89092 | <p>Symptom: When an administrator added bulk VLANs under Configuration > Network > VLAN > VLAN ID, the controller did not add the bulk VLANs and the web page displayed a JavaScript error. Correction in the formatting of the XML response from the controller to the WebUI fixed this issue.</p> <p>Scenario: This issue was observed in controllers running ArubaOS 6.4.</p> |
| 90110 | <p>Symptom: The ArubaOS Campus WLAN Wizard was not accessible. This issue is resolved by changing the LDAP server filter to include an ampersand (&).</p> <p>Scenario: The Campus WLAN wizard was not accessible due to the presence of an ampersand (&) in the LDAP server filter. This issue was observed in a 650 controller running ArubaOS 6.2.1.3, but could impact any controller model.</p> |
| 90264 | <p>Symptom: Layer 2 Tunneling Protocol (L2TP) pool was not displayed when the user-role was configured in the WebUI of a controller without an AP license. This issue is fixed by removing the WLAN_REMOTE_AP license validation while configuring L2TP pool.</p> <p>Scenario: This issue was triggered by Policy Enforcement Firewall (PEF) license with WLAN_REMOTE_AP validation while configuring L2TP pool on a controller. This issue was not limited to any specific controller model or release version.</p> |
| 92340 92649 | <p>Symptom: The WebUI of a controller failed to load in Internet Explorer 11 with the error message can't create XMLHttpRequest object: Object doesn't support property or method 'createXMLHttpRequest'. The ArubaOS WebUI is updated to be compatible with the new standards in Internet Explorer 11.</p> <p>Scenario: This issue was caused by changes in Internet Explorer 11 from Internet Explorer 10. This issue was observed in Internet Explorer 11 and not limited to any specific controller model or release version.</p> |
| 92620 | <p>Symptom: When TPM Initialization failed, the following error message was displayed: TPM Initialization or Certificate Initialization failed. For debug information see /tmp/deviceCertLib.log. The fix ensures that the error message points to the show tpm errorlog command.</p> <p>Scenario: This issue was observed when the Trusted Platform Module (TPM) Initialization or Certificate Initialization failed. This issue was not limited to a specific controller model.</p> |
| 93606 | <p>Symptom: Clients were not displayed in the Monitoring > Controller > Clients page of the WebUI when filtered with AP Name. This issue is fixed by changing the show user-table location <ap-name> command to show user-table ap-name <ap-name>.</p> <p>Scenario: This issue was triggered by changes to CLI commands. This issue was observed in controllers running ArubaOS 6.2 and 6.3.</p> |

WLAN Management System

Table 127: *WLAN Management System Fixed Issues*

| Bug ID | Description |
|--------|--|
| 84146 | <p>Symptom: WLAN Management System (WMS) slowed down with redundant database queries in a controller. This issue is fixed by ignoring queries to the database that determine if there are more Virtual APs (VAPs) present on the probe. Now, the information on VAP presence can be retrieved from the in-memory data structures.</p> <p>Scenario: This issue occurred when many APs rebooted, WMS marked them as down. This caused the WMS to slow down by generating redundant database queries. This issue was not limited to any specific controller model or release version.</p> |

XML API

Table 128: *XML API Fixed Issues*

| Bug ID | Description |
|--------|--|
| 84801 | <p>Symptom: Clients connected to the local controller were unable to access the Captive Portal (CP) page from an external server. This issue is resolved by configuring the default-xml-api parameter in the AAA profile.</p> <p>Scenario: This issue was observed when the default-xml-api was not configured. This issue was not limited to any specific controller or AP model.</p> |

This chapter describes the known and outstanding issues identified in ArubaOS 6.4.x release versions.

Known Issues and Limitations in ArubaOS 6.4.2.1

The following are the known issues and limitations found in ArubaOS 6.4.2.1. Applicable Bug IDs and workarounds are included.

Airgroup

Table 129: *Airgroup Fixed Issues*

| Bug ID | Description |
|--------|--|
| 106505 | <p>Symptom: Controller sends multiple authentication requests for AirGroup users to CPPM server when it does not receive a response from the CPPM server.</p> <p>Scenario: This issue is not limited to a specific controller model.</p> |

AP-Platform

Table 130: *AP-Platform Known Issues*

| Bug ID | Description |
|--------|--|
| 106096 | <p>Symptom: The radios of an AP-270 Series device are enabling after receiving power through PoE+ source.</p> <p>Scenario: An AP starts with power profile 2 and switches to profile 1 if 25.5W power is negotiated through Link Layer Discovery Protocol (LLDP). Prior to ArubaOS 6.4.2.0, LLDP negotiation starts immediately, and the AP switches power profile to 1 before it sends a Hello or Keep alive message to the controller. So, the controller is only aware that the AP is powered from a PoE+ source and radios are brought up normally. This behaviour changed in ArubaOS 6.4.2.0, and the LLDP negotiation starts only after the AP receives the configuration from the controller. The AP eventually receives PoE+ power but after sending the HELLO message the PoE flag. This issue is observed in AP-270 Series devices running ArubaOS 6.4.2.0.</p> <p>Workaround: After detecting change of power, resend the HELLO message with the updated power flag.</p> |

AP-Regulatory

Table 131: *AP-Regulatory Known Issues*

| Bug ID | Description |
|--------|--|
| 106698 | <p>Symptom: Some RF signals erroneously trigger RADAR events.</p> <p>Scenario: This issue is observed on AP-225 access points operating on Dynamic Frequency Selection (DFS) channels and running ArubaOS 6.4.1.0.</p> <p>Workaround: None.</p> |

AP Wireless

Table 132: *AP Wireless Known Issues*

| Bug ID | Description |
|----------------------------|---|
| 98692 | Symptom: AP-220 Series access points running ArubaOS 6.4.0.2 stops responding and reboots. The log files for the event lists the reason for the crash as kernel panic: Fatal exception . Scenario: This issue occurs on 7210 Series controllers in a master-local topology where AP-200 Series access points terminate on both the controllers in campus mode. Workaround: Memory improvements in ArubaOS resolved the issue. Duplicate Bugs: The following bug IDs have reported similar issues: 99914, 100459, 101167, 101862, 103013, 106065 |
| 100371 104827 105613 | Symptom: Communication badges fail to connect to AP-225 access point intermittently. Scenario: This issue is observed in Vocera communication badges trying to connect to AP-225 access points running ArubaOS 6.3.1.6. |
| 102639 | Symptom: Windows Surface RT tablets do not connect to 802.11w capable SSID with 802.1x authentication AES encryption. Scenario: This issue occurs when Enable 802.11w Management Frame Protection is set to Capable or Required . Workaround: Disable MFP capability. |
| 105089 | Symptom: The wireless clients experienced packet loss when connected to the AP-135 where the multicast is using Dynamic Multicast Optimization (DMO). Scenario: This issue is observed in AP-135 where the DMO enables an SSID profile and the client does not send ACK pack when receiving high 11n rate data. Workaround: Reduce retry tx data rate on the AP. |
| 105941 | Symptom: Users are unable to complete file downloads on their hand-held devices due to performance issues. Scenario: This issue is observed on devices connected to AP-225 and 7210 controllers running ArubaOS 6.4.1.0, 6.3.1.1, and 6.3.1.9. Workaround: None. |

Controller-Datapath

Table 133: *Controller-Datapath Known Issues*

| Bug ID | Description |
|--------|---|
| 88629 | Symptom: ACL enforcement for Microsoft® Skype doesn't work consistently. Scenario: This issue occurs on 7200 Series controllers running ArubaOS 6.4 when Deep Packet Inspection (DPI) is enabled on the controller. Workaround: None. |
| 89722 | Symptom: Facebook® application traffic is not getting classified correctly. Scenario: This issue occurs on 7200 Series controllers running ArubaOS 6.4 when DPI is enabled on the controller. Workaround: None. |
| 92955 | Symptom: When sending small sized data packets at high speed data rate through IPSec tunnel, the controller crashes due to datapath timeout . Scenario: This issue is observed when the controller sends IPSec traffic at 400 Mbps with 64 bytes packet size. This causes the controller's ingress queue run out of buffer. This issue is not limited to a specific controller model or software release version. Workaround: None. |

Controller-Platform

Table 134: *Controller-Platform Known Issues*

| Bug ID | Description |
|--------|--|
| 105625 | Symptom: The gunzip module crashes after the controller is upgraded to ArubaOS 6.4.1.0 Scenario: This issue is observed in 6000 controllers running ArubaOS 6.4. Workaround: None. |
| 105903 | Symptom: The gunzip module crashes after the controller is upgraded to ArubaOS 6.4.1.0 Scenario: This issue occurs in 7000 Series controllers running ArubaOS version 6.4.2.0 or later. Workaround: None. |

HA-Lite

Table 135: *HA-Lite Known Issues*

| Bug ID | Description |
|--------|--|
| 106070 | Symptom: AP fails to create standby tunnel with standby controller. Scenario: This issue occurs when AP reboots because of a missed heartbeat with the active controller and the IP address of BLMS and IP address of standby controller is the same. Workaround: Do not configure BLMS in ap system-profile . |

Local Database

Table 136: *Local Database Known Issues*

| Bug ID | Description |
|--------|--|
| 105626 | Symptom: A time out occurs when authenticating a client on a local controller against the local database on a master controller. Scenario: This issue is observed in master-local configuration with clients on the local controller authenticating against the local database on a master controller running ArubaOS 6.4.1.0. Workaround: Use the local database on the local controller by configuring the use local switch internal-db command on the local controller. |

LLDP

Table 137: *LLDP Known Issues*

| Bug ID | Description |
|--------|--|
| 94647 | Symptom: In rare cases, a lldp GSM PORT_INFO Lookup failed at Function: sm_handle_lldp_info_events error message appears in the log. Scenario: This issue occurs when the script to shut or open the interface is executed multiple times. This issue is not limited to any specific controller model and occurs on ArubaOS running 6.4. Workaround: None. |

Mobility

Table 138: *Mobility Known Issues*

| Bug ID | Description |
|--------|---|
| 105902 | <p>Symptom: iOS and Android devices randomly fail to pass traffic over a wireless network.</p> <p>Scenario: This issue is seen under the following scenario:</p> <ul style="list-style-type: none">• The clients connect to the 802.1X SSID.• There is a VLAN ID mis-match of the route-cache table and the association table. <p>This issue is observed in 3600 and 6000 controllers in a master-local topology running ArubaOS 6.3.1.8, 6.4.1.0, or 6.4.2.0.</p> <p>Workaround: None.</p> |

Remote AP

Table 139: *Remote AP Known Issues*

| Bug ID | Description |
|--------|--|
| 105794 | <p>Symptom: The output of the show iap table command displays the status of an IAP as DOWN on the controller though the VPN status shows that the IAP is UP.</p> <p>Scenario: This issue is observed because the MAC address of the IAP is missing in the trusted database of the controller running ArubaOS 6.4.</p> <p>Workaround: None.</p> |

Voice

Table 140: *Voice Known Issues*

| Bug ID | Description |
|--------|--|
| 87316 | <p>Symptom: The Call Detailed Record (CDR) for a VoIP client goes into ABORTED state due to session age out.</p> <p>Scenario: This issue is observed in an L3 mobility deployment when the Real-time Transport Protocol (RTP) packets do not get tunneled to the Home Agent (HA), when a client that has roamed to the Foreign agent (FA) initiates a Lync call. This issue is observed in controllers running ArubaOS 6.3 or later versions.</p> <p>Workaround: None.</p> |

WebUI

Table 141: *WebUI Known Issues*

| Bug ID | Description |
|----------------|--|
| 97789 98763 | <p>Symptom: Controllers running ArubaOS 6.4 or later versions fail to copy an ArubaOS image using Windows TFTP.</p> <p>Scenario: This issue is seen when you copy an ArubaOS image onto the non-boot partition of the controller using TFTP. The following error message is displayed:</p> <ul style="list-style-type: none">• In WebUI: Error determining new default boot partition version <p>This issue is not limited to any specific controller model and observed in controllers running ArubaOS 6.4 or later versions.</p> <p>Workaround: Use FTP or SCP to copy an ArubaOS image onto the non-boot partition.</p> |

Wi-Fi Multimedia

Table 142: *Wi-Fi Multimedia Known Issues*

| Bug ID | Description |
|--------|---|
| 101501 | Symptom: The quality of Lync calls are bad and MOS score is low when there are 15 clients in power saving mode and another 15 clients receive downstream UDP traffic at 10 MBPS in each client. Scenario: This issue is observed in AP-200 Series and AP-220 Series in tunnel and decrypt tunnel forwarding mode running ArubaOS 6.3.1.8, 6.4.0.3, or 6.4.1.0. Workaround: None. |

Known Issues and Limitations in ArubaOS 6.4.2.0

The following are the known issues and limitations found in ArubaOS 6.4.2.0. Applicable Bug IDs and workarounds are included.

AP Wireless

Table 143: *AP Wireless Known Issues*

| Bug ID | Description |
|------------------|--|
| 103545 | Symptom: Traffic is not flowing when users are connected in the bridge mode. The user is unable to access the internet or intranet server or any host on the same subnet. User is able to get an IP address at times, but the IP address does not up in user table. This issue occurs when the customer upgrades the controller to ArubaOS 6.4.1.0. Scenario: This issue occurs in M3 Series controllers running ArubaOS 6.4.1.0. Workaround: None. |
| 103810 104199 | Symptom: Following a successful association users are deauthenticated with reason Denied; Internal Error . This issue is seen intermittently after the controller is upgraded from ArubaOS 6.4.0.3 to 6.4.1.0. Scenario: This issue occurs on 7220 controllers running ArubaOS 6.4.1.0. Workaround: None. |
| 103991 104507 | Symptom: Multicast video stream freezes on Windows Media Player clients. Scenario: This issue occurs when the number of clients on an AP scales beyond 20. Workaround: Reduce energy drop timeout of 5 GHz to the same value as 2 GHz. |

AP Platform

Table 144: *AP Platform Known Issues*

| Bug ID | Description |
|------------------|--|
| 104218 101794 | Symptom: An sapd process crashes while running Microsoft Request For Information (RFI) tests. Scenario: This issue is observed in AP-225 access points running ArubaOS 6.4.0.3. The crash is caused by zero length Fast Fourier Transforms (FFTs). Workaround: This issue is resolved by disabling spectrum-monitoring in the AP mode or disabling spectrum-mode. |

Controller-Datapath

Table 145: *Controller-Datapath Known Issues*

| Bug ID | Description |
|---|--|
| 95706 100817 102229 103914 104137 | Symptom: A 7200 Series controller unexpectedly stops passing network traffic. Scenario: This issue is triggered by a hardware error on a 7200 Series controller using auto negotiated Ethernet speeds. Workaround: Manually define ethernet speeds for each port on the 7200 Series controller. |

Policy Based Routing

Table 146: *Policy Based Routing Known Issues*

| Bug ID | Description |
|--------|---|
| 104169 | Symptom: The user is unable to add SRC-NAT using the Web UI when the ESI policy is enabled. Scenario: This issue is observed in ArubaOS 6.3.x and 6.4.x. Workaround: The user can configure SRC-NAT using the CLI, when ESI Policy is enabled. |

WebCC

Table 147: *WebCC Known Issues*

| Bug ID | Description |
|--------|--|
| 104189 | Symptom: The WebCC process crashes randomly with SIGSEGV fault Scenario: This issue was observed when enabling and disabling the WebCC feature repeatedly in quick succession. This issue was observed on 7200 Series and 7000 Series controllers running ArubaOS 6.4.2. Workaround: The WebCC process restarts and recovers automatically. However, crash info is available during restart or when the show switchinfo command is executed. |

Known Issues and Limitations in ArubaOS 6.4.1.0

The following are the known issues and limitations found in ArubaOS 6.4.1.0. Applicable Bug IDs and workarounds are included.

AP Regulatory

Table 148: *AP Regulatory Known Issues*

| Bug ID | Description |
|--------|---|
| 99290 | Symptom: 80 MHz channels in the Hong Kong regulatory domain are disabled on the AP-220 Series. Scenario: 80 MHz channels are not supported on the AP-220 Series within the Hong Kong regulatory domain. Workaround: Download and activate the latest regulatory file from the Aruba support site. |
| 102555 | Symptom: The Puerto Rico regulatory domain is disabled on the AP-270 Series. Scenario: The AP-270 Series is not currently supported in the Puerto Rico regulatory domain. Workaround: Enable the US regulatory domain or download and activate the latest regulatory file from the Aruba support site. |

Controller-Datapath

Table 149: *Controller-Datapath Known Issues*

| Bug ID | Description |
|--------|--|
| 93327 | Symptom: World of Warcraft® online game sessions are not getting classified correctly. Scenario: This issue occurs on 7200 Series controllers running ArubaOS 6.4 when AppRF is enabled on the controller. Workaround: None |
| 100359 | Symptom: Clients using phones connected to wired ports of RAPs experience poor call quality. Scenario: This issue is observed with RAP-2WG, RAP-3WN, and RAP-5WN running ArubaOS 6.3.1.0. Workaround: None. |
| 101010 | Symptom: When both DMO and broadcast-filter-all is enabled and port-channel is used for uplink port, incoming known multicast traffic from uplink is dropped in the controller. Scenario: This issue occurs in controllers running ArubaOS 6.3.x.0 and 6.4.x.0. Workaround: None. |

Remote AP

Table 150: *Remote AP Known Issues*

| Bug ID | Description |
|--------|---|
| 101962 | Symptom: Remote AP (RAP) shows the status as down on the controller when custom certificate is configured on the RAP. Scenario: A USB containing a pfx file is connected to the RAP. During boot up, the RAP searches for the pfx file and loads the key/certificates from the pfx file. The key/certificates are used in IKEv2 tunnel establishment. When the USB has more than one pfx file in different directories having a same file name such as <mac-address>.p12, the RAP fails to upload the pfx files and hence cannot establish an IKEv2 tunnel. This issue is not specific to any controller model or ArubaOS release version. Workaround: On the USB connected to the RAP, delete any duplicate pfx file. Only one pfx file must be present with the RAP MAC address i.e., <mac-address>.p12. |

WebUI

Table 151: *WebUI Known Issues*

| Bug ID | Description |
|--------|---|
| 97710 | Symptom: The WebUI displays the error, can't do cli:SID validation failed when a client logs in after upgrading the controller using the WebUI. Scenario: This issue is not limited to any specific controller model. Workaround: Clear the browser cache after the image is upgraded. |
| 101390 | Symptom: Using the controller's WebUI, a user cannot copy files to a USB drive connected to slot 1 of the controller. Scenario: There are two USB slots in 7010 controller. This issue is observed in 7010 controller running ArubaOS 6.4.1.0. Workaround: Use the CLI to copy files to a USB drive connected to slot 1 of the controller. Or To copy files, connect the USB drive to slot 0 of the 7010 controller. |

Known Issues and Limitations in ArubaOS 6.4.0.2

The following are the known issues and limitations in ArubaOS 6.4.0.2. Applicable Bug IDs and workarounds are included.

AP-Wireless

Table 152: *AP-Wireless Known Issues*

| Bug ID | Description |
|--------|---|
| 88940 | Symptom: A crash is observed on APs when the status of the channel is set inappropriately by the process handling the AP management. Scenario: This issue is observed when a standard RAP or CAP is configured at the Dynamic Frequency Selection (DFS) channel. This issue is observed in AP-70 connected to controllers running ArubaOS 6.3.1.2. Workaround: Set the AP channel to No DFS before rebooting the AP. |
| 97333 | Symptom: All clients associated with an AP disassociates when more than 48 users start FTP downloads. Scenario: This issue is observed on controllers running ArubaOS 6.4.0.1. Workaround: None. |

Base OS Security

Table 153: *Base OS Security Known Issues*

| Bug ID | Description |
|--------|--|
| 93550 | Symptom: Running the aaa test-server command for a TACACS authentication server displays AAA server timeout in spite of successful authentication. Scenario: This issue is not limited to a specific controller model or release version. Workaround: Issue the aaa test-server command twice. |

Controller-Datapath

Table 154: *Controller-Datapath Known Issues*

| Bug ID | Description |
|--------|--|
| 91085 | Symptom: Google® hangout sessions are classified as Google. Scenario: This issue occurs on 7200 Series controllers running ArubaOS 6.4 when AppRF is enabled on the controller. Workaround: None. |

Controller-Platform

Table 155: *Controller-Platform Known Issues*

| Bug ID | Description |
|--------|---|
| 94615 | <p>Symptom: The controller may get into an OutOfMemory or kernel panic state during an ArubaOS image upgrade.</p> <p>Scenario: This issue is seen when you issue the tar logs tech-support command repetitively on the controller. This depletes the kernel LowFree memory. This issue is observed in 600 Series controller running ArubaOS 6.4 or later versions.</p> <p>Workaround: Do not issue the tar logs tech-support command repetitively before upgrading an ArubaOS software image.</p> |

LLDP

Table 156: *LLDP Known Issues*

| Bug ID | Description |
|--------|---|
| 94302 | <p>Symptom: In rare cases, issuing some of the LLDP show commands display the <ERRS> lldp Invalid Physical Port 0 passed at Function: li_get_handle error message in the log. This issue does not impact any functionality.</p> <p>Scenario: This issue is not specific to any controller model and occurs on ArubaOS running 6.4.</p> <p>Workaround: None.</p> |

PhoneHome

Table 157: *PhoneHome Known Issues*

| Bug ID | Description |
|--------|---|
| 96219 | <p>Symptom: Issuing the no phonehome smtp command removes SMTP as the transport protocol but does not rollback to the default HTTPS mode.</p> <p>Scenario: This issue is seen when you delete SMTP as the transport protocol. This issue is observed in controllers running ArubaOS 6.4 or later versions.</p> <p>Workaround: To roll back to the default HTTPS mode, issue the phonehome https <email address> command.</p> |

Startup Wizard

Table 158: *Startup Wizard Known Issues*

| Bug ID | Description |
|--------|---|
| 98110 | <p>Symptom: Mobility Controller Setup Wizard page gets stuck with Java script error when you click Next on the VLANs and IP Interfaces tab of the controller's WebUI.</p> <p>Scenario: This issue is not limited to any specific controller model and is observed in ArubaOS 6.4.0.2.</p> <p>Workaround: Use Mozilla® Firefox browser to access the VLANs and IP Interfaces tab of the Setup Wizard page.</p> |
| 98159 | <p>Symptom: Campus WLAN Wizard page gets stuck in Role Assignment step when you click Next on the Authentication Server step of the controller's WebUI using Microsoft® Internet Explorer 10 or Internet Explorer 11.</p> <p>Scenario: This issue is not limited to any specific controller model and is observed in ArubaOS 6.4.0.2.</p> <p>Workaround: Use any browser other than Internet Explorer 10 and Internet Explorer 11 to access the Role Assignment tab under the Setup Wizard page.</p> |

Known Issues and Limitations in ArubaOS 6.4.0.1

The following are the known issues and limitations found in ArubaOS 6.4.0.1. Applicable Bug IDs and workarounds are included.

PhoneHome

Table 159: *PhoneHome Known Issues*

| Bug ID | Description |
|--------|--|
| 96901 | Symptom: The auto-report of the PhoneHome statistics is displayed incorrectly in the show phonehome stats command output though the report is sent successfully. Scenario: This issue occurs when auto-report is triggered from support mode. This issue is observed in controllers running ArubaOS 6.4.0.1. Workaround: None. |

Known Issues and Limitations in ArubaOS 6.4.0.0

The following are known issues and limitations in ArubaOS 6.4.0.0. Applicable Bug IDs and workarounds are included.

AirGroup

Table 160: *AirGroup Known Issues*

| Bug ID | Description |
|--------|--|
| 91690 | Symptom: Clients were unable to use AirGroup services to connect to other iChat clients. Scenario: This issue was observed in ArubaOS 6.3.0.1, and is triggered because AirGroup does not support unsolicited advertisements required by iChat. As a result, clients are unable to immediately discover each other when they log in to the network using Bonjour. Workaround: None. |
| 94208 | Symptom: Wireless Clients such as iPad and iPhone running the SONOS® Controller application do not discover the SONOS music system. Scenario: This issue is observed when AirGroup is enabled on a controller with the SONOS music system connected. Workaround: None. |

AP-Platform

Table 161: *AP-Platform Known Issues*

| Bug ID | Description |
|----------------|---|
| 91172 | Symptom: A controller crashes occasionally during freeing some corrupted memory packets. Scenario: This issue is not limited to any specific controller model or release version. Workaround: None. |
| 93876 | Symptom: Occasionally, the CPSEC CAPs unexpectedly reboot. Scenario: This issue occurs on all AP platforms with CPSEC and CAPs and may be caused by IKEv2 timing out. Workaround: None. |
| 91805 93963 | Symptom: An AP reboots occasionally without reboot reason or crash information. Scenario: This issue occurs on the AP-125 running ArubaOS 6.3.0.1. Workaround: None. |
| 95056 | Symptom: An AP-120 Series device crashes with the log message Unhandled kernel unaligned access . Scenario: This issue occurs on AP-120 Series models running ArubaOS 6.3.1.2. Workaround: None. |
| 95260 | Symptom: An AP occasionally reboots with crash information cache_alloc_refill . Scenario: This issue occurs on the AP-120 Series models running ArubaOS 6.3.1.2. Workaround: None. |
| 95764 | Symptom: An AP-125 device crashes and reboots, the log files for the event list the reason for the crash as Kernel unaligned instruction access . Scenario: This issue occurs in AP-125 access points connected to controllers running ArubaOS 6.3.1.2. Workaround: None. |

AP-Wireless

Table 162: *AP-Wireless Known Issues*

| Bug ID | Description |
|---|---|
| 69424 71334 74646 75248 75874 | Symptom: When upgraded to ArubaOS 6.2, AP-125 crashes and reboots. Scenario: This issue is observed when upgrading to ArubaOS 6.2 from ArubaOS 6.1.3.2 and later in any deployment with an AP-125. Workaround: None. Duplicate Bugs: The following bug IDs have reported similar issues: 78978, 78981, 79891, 80054, 85753, 87250, 87360, 88619, 88620, 88989, 89537, 91689, 92641, 92975, 93079, 93455, 93811, 91689 |
| 86184 | Symptom: Wireless clients are unable to associate to an access point on the 5GHz radio. Scenario: This issue is observed when a channel change in an access point fails after a Dynamic Frequency Selection (DFS) radar signature detection. This issue is observed in AP-125 running ArubaOS 6.1.x, 6.2.x, 6.3.x, and 6.4.x. Workaround: None. |
| 91510 | Symptom: An access point reboots occasionally without reboot reason or crash information. Scenario: This issue occurs on AP-134 and AP-135 connected to controllers running ArubaOS 6.3.0.1. Workaround: None. |

Table 162: *AP-Wireless Known Issues*

| Bug ID | Description |
|---|--|
| 93380 93494 93687 93744 | <p>Symptom: Occasionally, an AP stops responding and reboots.</p> <p>Scenario: This issue is observed because of the Ethernet connectivity problem leading to loss of connectivity between the AP and controller. This issue occurs on AP-224 and AP-225 models and is not limited to a specific ArubaOS version.</p> <p>Workaround: Ensure that the Ethernet connection issue does not lead to loss of connectivity between the AP and the controller.</p> |
| 93511 93953 | <p>Symptom: The user gets error Could not read cached limits and License number mismatch in cached limits messages in a controller with master-local topology.</p> <p>Scenario: This issue is not limited to any specific controller model and is observed in controllers running ArubaOS 6.3 or later.</p> <p>Workaround: None.</p> |
| 95113 95086 95088 95111 95114 | <p>Symptom: An iPad connected in tunnel mode using CCMP encryption becomes unreachable from the network once Airplay mirroring is initiated from iPad to Apple TV.</p> <p>Scenario: This issue occurs when an iPad is connected to a wireless network in forward-mode: Tunnel and opmodes: wpa2-aes/wpa2-psk-aes. This issue is observed in controllers and APs running ArubaOS 6.3.x.x or 6.4.x.x.</p> <p>Workaround: Disable Multiple Tx Replay Counters parameter under SSID profile.</p> <p>Duplicate Bugs: The following bug IDs have reported similar issues: 95115, 95116, 95117, 95123, 95124</p> |

Base OS Security

Table 163: *Base OS Security Known Issues*

| Bug ID | Description |
|--------|--|
| 93550 | <p>Symptom: Running the aaa test-server command for a TACACS authentication server displays AAA server timeout in spite of successful authentication.</p> <p>Scenario: This issue is not limited to a specific controller model or software release version.</p> <p>Workaround: Issue the aaa test-server command twice.</p> |
| 95449 | <p>Symptom: A controller reboots and displays the message Reboot Cause: Nanny rebooted machine - fpapps process died.</p> <p>Scenario: This issue may occur in M3 controllers running ArubaOS 6.3 in a master-local topology.</p> <p>Workaround: None.</p> |

Captive Portal

Table 164: *Captive Portal Known Issues*

| Bug ID | Description |
|--------|--|
| 92927 | <p>Symptom: When Apple® clients try to access a web page using captive portal, the controller displays error occurred message on the client's browser.</p> <p>Scenario: This issue is observed in a Virtual AP (VAP)-SSID enabled network with external captive portal authentication. Further investigation suggested that the backslash (\) character is not URL-encoded. As a result, external captive portal stops working for Apple clients.</p> <p>Workaround: None.</p> |

Configuration

Table 165: *Configuration Known Issues*

| Bug ID | Description |
|--------|--|
| 93922 | <p>Symptom: A custom banner with the # delimiter gets added as part of the show running-config command output.</p> <p>Scenario: The issue is observed when an administrator configures the banner using the banner motd command in the controller with the # delimiter. This issue is not limited to a specific controller model and is observed in ArubaOS 6.3.1.1 or later versions.</p> <p>Workaround: None.</p> |

Controller-Datapath

Table 166: *Controller-Datapath Known Issues*

| Bug ID | Description |
|--------|--|
| 91085 | <p>Symptom: Google hangout sessions are classified as Google when AppRFv2 is enabled.</p> <p>Scenario: This issue occurs on 7200 Series controllers running ArubaOS 6.4.</p> <p>Workaround: None.</p> |
| 92248 | <p>Symptom: A crash occurs on a master controller and the log files for the event listed the reason for the crash as datapath timeout.</p> <p>Scenario: The trigger of this issue is not known and this issue is observed in 3400 controllers running ArubaOS 6.3.1.0 in a master-local topology.</p> <p>Workaround: None.</p> |
| 92477 | <p>Symptom: Bittorrent sessions are not denied only when the deny rule is added in the middle of a bittorrent file download.</p> <p>Scenario: This issue occurs because the bittorrent control session information is deleted once the traffic is classified. This issue occurs on 7200 Series controllers when DPI is set to On.</p> <p>Workaround: Creating a bittorrent rule in the user role before a bittorrent file download denies the bittorrent traffic.</p> |
| 93285 | <p>Symptom: An M3 controller reboots unexpectedly. The log files for the event listed the reason as datapath timeout.</p> <p>Scenario: This issue occurs in M3 controllers running ArubaOS 6.3.X.X.</p> <p>Workaround: None.</p> |
| 93582 | <p>Symptom: A 7210 controller crashes. The logs for this error listed the reason for the crash as datapath timeout.</p> <p>Scenario: This issue is observed in 7210 controllers running ArubaOS 6.3.1.0.</p> <p>Workaround: None.</p> |
| 93817 | <p>Symptom: The master controller throws an internal error while provisioning APs that belong to a specific local controller.</p> <p>Scenario: This issue occurs on 3200 controllers running ArubaOS 6.3.1.1 in a master-local topology.</p> <p>Workaround: None.</p> |
| 94143 | <p>Symptom: A 3200 controller reboots unexpectedly. The log files for the event listed the reason as datapath timeout.</p> <p>Scenario: This issue is observed on a 3200 controller running ArubaOS 6.3.1.1.</p> <p>Workaround: None.</p> |

Table 166: *Controller-Datapath Known Issues*

| Bug ID | Description |
|-------------------------|---|
| 93203 94200 | <p>Symptom: A local controller reboots unexpectedly. The log files for the event listed the reason for the reboot as datapath exception.</p> <p>Scenario: This issue is observed in 7220 controller running ArubaOS 6.3.1.1 in a master-local topology.</p> <p>Workaround: None.</p> |
| 94267 | <p>Symptom: After an upgrade to ArubaOS 6.3.1.x, clients unexpectedly disconnected from the network, or were unable to pass traffic for 2-3 minutes after roaming between APs.</p> <p>Scenario: This issue was observed in Psion Omni handheld scanners roaming between AP-175 and AP-120 Series APs running ArubaOS 6.3.1.1.</p> <p>Workaround: None.</p> |
| 94636 | <p>Symptom: A crash occurs on a local controller and the log files for the event listed the reason for the crash as datapath timeout.</p> <p>Scenario: The trigger of this issue is not known and this issue is observed in 7210 controllers running ArubaOS 6.3.0.1.</p> <p>Workaround: None.</p> |
| 93203 94965 95719 | <p>Symptom: A 7210 controller crashes. The logs for this error listed the reason for the crash as datapath timeout.</p> <p>Scenario: The trigger of this issue is not known and this issue is observed in 7210 controllers running ArubaOS 6.3.1.1 in a master-local topology.</p> <p>Workaround: None.</p> |
| 95286 | <p>Symptom: A master controller crashes with log message datapath timeout.</p> <p>Scenario: The trigger of this issue is unknown and is observed in 7220 controllers running ArubaOS 6.3.1.1.</p> <p>Workaround: None.</p> |

Controller-Platform

Table 167: *Controller-Platform Known Issues*

| Bug ID | Description |
|---|---|
| 80200 81225 81752 81930 84672 | <p>Symptom: The 600 Series and 3000 Series controllers reboots with kernel panic.</p> <p>Scenario: This issue is observed because of high traffic in control plane for a sustained period. This issue occurs on 600 Series and 3000 Series controllers running ArubaOS 6.3.0.0 or later.</p> <p>Workaround: Configure bandwidth contracts depending on the incoming traffic.</p> <p>Duplicate Bugs: The following bug IDs have reported similar issues: 85422, 87079, 89014, 89243, 89726</p> |
| 92968 | <p>Symptom: Generating the tech-support.log file from the WebUI of the controller gets truncated at times. Scenario: This issue is not limited to a specific controller model and is observed in ArubaOS 6.2.1.3, ArubaOS 6.3.1.0 or later versions.</p> <p>Workaround: Issue the tar logs tech-support command from the CLI to download the tech-support.log file.</p> |
| 93465 | <p>Symptom: A local controller reboots unexpectedly. The log files for the event listed the reason for the reboot as Control Processor Kernel Panic.</p> <p>Scenario: This issue occurs when the controller releases the memory of corrupted data packets. This issue is observed in 3000 Series and M3 controllers running ArubaOS 6.3.1.1 in a master-local topology.</p> <p>Workaround: None.</p> |

Table 167: *Controller-Platform Known Issues*

| Bug ID | Description |
|--------|--|
| 94862 | Symptom: The master controller reboots unexpectedly with the message: "user reboot (shell)." Scenario: This issue occurs on the 7200 Series controllers with AP-225 APs following an upgrade to ArubaOS 6.4. Workaround: None. |
| 95071 | Symptom: Issuing a show command from the CLI of a standby controller running ArubaOS 6.3.1.1 triggers the error "Module Configuration Manager is Busy" Scenario: This issue was observed in a standby 3600 controller in a master-standby topology, Workaround: None. |

DHCP

Table 168: *DHCP Known Issues*

| Bug ID | Description |
|--------|---|
| 94345 | Symptom: The Symbol N410 and Android devices do not receive an IP address from the internal DHCP Server. Scenario: This issue is observed on controllers running ArubaOS 6.3.1.1 and occurs when the controller's internal DHCP is configured to serve IP addresses for these devices. Workaround: Use an external DHCP server. |
| 95166 | Symptom: When a controller is configured as a DHCP server, by default it attempts Dynamic DNS updates and the following log message appears: "dhcpd: if CU-iPad-2-64-GB.aspect.com IN A rrset doesn't exist add CU-iPad-2-64-GB.aspect.com 10800 IN A 169.136.135.108: destination address required." Scenario: This issue is observed on controllers running ArubaOS 6.3 and later. It is caused when the DHCPD server issues a DHCP address and then attempts a DDNS update. Workaround: None. |

Hardware-Management

Table 169: *Hardware-Management Known Issues*

| Bug ID | Description |
|----------------|--|
| 87191 87808 | Symptom: A controller unexpectedly stops responding and reboots. Scenario: This issue is observed when a module (hwMon) crashes on the controller. This issue occurs on M3 series controllers running ArubaOS 6.3.0.1 or later. Workaround: None. |

IPSec

Table 170: *IPSec Known Issues*

| Bug ID | Description |
|--------|---|
| 80460 | Symptom: Remote client and Site-to-Site VPN performance is low and does not scale to the controller limit when IKEv2 with GCM256-EC384 encryption algorithm configured. Scenario: This issue is observed on 600 Series, 3000 Series, and M3 controllers and occurs when the IKE session is established to a standby unit in a failover deployment. Workaround: None. |
| 95634 | Symptom: Site-to-Site IPsec VPN tunnels randomly lose connectivity on a 7210 controller. Scenario: This issue is observed where there are 500 or more remote sites terminating IPsec VPN tunnels on a 7210 controller. This issue is observed on a 7210 controller running ArubaOS 6.3.1.2. Workaround: None. |

Local Database

Table 171: *Local Database Known Issues*

| Bug ID | Description |
|--------|---|
| 95277 | Symptom: The Remote AP whitelist on a master controller is not correctly synchronizing entries to local controllers. Scenario: This issue occurs in ArubaOS 6.3.x.x when the description field of a remote whitelist entry contains an apostrophe ('). Workaround: Remove the apostrophe from the whitelist entry description. |

LLDP

Table 172: *LLDP Known Issues*

| Bug ID | Description |
|--------|---|
| 92998 | Symptom: The remote interface name appears as Not received while issuing the show lldp neighbor command. Scenario: This issue occurs when Link Layer Discovery Protocol (LLDP) is enabled on the controller and if the neighbor is a third-party device such as Arista or Alcatel. This issue is not specific to any controller model and occurs on ArubaOS running 6.4. Workaround: None. |

Master-Local

Table 173: *Master-Local Known Issues*

| Bug ID | Description |
|--------|---|
| 88430 | Symptom: User-role configuration is lost after upgrading master, standby, and local controllers to ArubaOS 6.3.1 or later versions. Scenario: This issue is observed on a 7200 Series controller running ArubaOS 6.3.1 or later versions. Workaround: Disabling the configuration snapshot by executing the cfgm set sync-type complete command on master and standby controllers prevents partial configuration loss. Wait at least five (5) minutes after the upgraded master and standby have rebooted before reloading the upgraded local controller. |
| 88919 | Symptom: Global configuration like user-role on the master controller does not synchronize with the local controller after issuing the write memory command. Scenario: This issue is observed in a master-local topology. This issue is observed in 7200 Series controller running ArubaOS 6.3.0.0 or later versions. Workaround: On the master controller, issue the cfgm set sync-type complete command, followed by the write memory command to send the complete configuration file to the local controller. |

RADIUS

Table 174: *RADIUS Known Issues*

| Bug ID | Description |
|--------|---|
| 94081 | Symptom: Multiple authentication failures are observed in the controllers. Scenario: This issue is observed when external LDAP server is used for authentication. This issue is not limited to a specific controller models and occurs in ArubaOS running 6.3.x versions. Workaround: Reduce LDAP timeout parameter value to 3 seconds for LDAP servers. |

Remote AP

Table 175: *Remote AP Known Issues*

| Bug ID | Description |
|--------|---|
| 95572 | Symptom: Wired clients are unable to access the internet when connected to a Remote AP (RAP). Scenario: This issue is observed when wired clients cannot pass traffic locally with source NAT in split-tunnel forwarding mode. This issues is observed when the 3200 controller is upgraded from ArubaOS 6.1.3.6 to ArubaOS 6.3.1.2. Workaround: None. |
| 95658 | Symptom: Cisco® Unified IP Phone 7945G reboots randomly during an active voice call. Scenario: This issue is observed when a Cisco Unified IP Phone 7945G is connected to a Power over Ethernet (PoE) port of a RAP-3WNP remote AP. This issues is observed in ArubaOS 6.3.0.1. Workaround: None. |

Station Management

Table 176: *Station Management Known Issues*

| Bug ID | Description |
|---|---|
| 85662 84880 88009 88319 89321 | <p>Symptom: The state of APs are displayed as down on the master controller even if these APs are connected and UP.</p> <p>Scenario: This issue is observed when AP's system profile has a local controller as the primary Local Management Switch (Primary-LMS) and master controller is configured as a backup Local Management Switch (Backup-LMS). This issue is not limited to any specific controller model and occurs in ArubaOS running 6.3 or later.</p> <p>Workaround: Remove master controller as backup LMS during initial phase.</p> <p>Duplicate Bugs: The following bug IDs have reported similar issues: 92164, 93243, 93388, 93389, 93984</p> |
| 91758 | <p>Symptom: Stationary Apple® MacBook laptops unexpectedly disassociated from APs, and were temporarily unable to pass traffic for 3-5 minutes during a period when many users on the network were roaming between APs.</p> <p>Scenario: This issue occurs on a network with a controller running ArubaOS 6.3.1.1 with ARM channel assignment and scanning features enabled.</p> <p>Workaround: Disable ARM channel assignment and scanning features.</p> |

Voice

Table 177: *Voice Known Issues*

| Bug ID | Description |
|--------|--|
| 90888 | <p>Symptom: The show voice real-time-analysis command does not display any result for voice calls between Microsoft® Lync clients.</p> <p>Scenario: This issue is observed when Microsoft Lync clients are connected to the same Remote AP (RAP) in split-tunnel forwarding mode. In such a case, the voice packets are locally routed through the RAP without forwarding it to the controller. As a result, the controller does not display any Real-time Transport Analysis (RTPA) report. This issue is observed in controllers running ArubaOS 6.4.</p> <p>Workaround: None.</p> |

WebUI

Table 178: *WebUI Known Issues*

| Bug ID | Description |
|--------|--|
| 90026 | Symptom: When a user attempts to access the controller WebUI, the WebUI returns the Session Invalid error message. Scenario: The user is forced to attempt to access the WebUI two to three times before successfully logging in. Each failed attempt returns the Session Invalid error message. This error occurs on controllers running ArubaOS 6.3.0.1. Workaround: None. |
| 93454 | Symptom: The Dashboard > Spectrum page of the WebUI is not loading and re-subscription fails frequently. Scenario: This issue is observed in AP-105 access points associated to controllers running ArubaOS 6.3.0.1. Workaround: Use the ap spectrum clear-webui-view-settings command to avoid this issue. |
| 95185 | Symptom: Collecting the logs.tar and tech-support logs from the controller's WebUI fails with Error running report... Error: receiving data from CLI, interrupted system call error message. Scenario: This issue is not seen under the following cases: <ul style="list-style-type: none">• Downloading the logs.tar without the tech-support log from the WebUI.• Downloading the logs.tar and tech-support logs from the CLI. This issue is observed in 7220 controller running ArubaOS 6.3.1.2. Workaround: Download the logs.tar and tech-support logs from the CLI. |

Issues Under Investigation

The following issues have been reported in ArubaOS 6.4.x and are being investigated.

AP-Wireless

Table 179: *AP-Wireless Issues Under Investigation*

| Bug ID | Description |
|--------|---|
| 106120 | Symptom: Users are unable to associate to AP-205 with more than one Single-Spatial Stream. However, same client connects to AP-125 with two Single-Spatial Stream. |

Controller-Datapath

Table 180: *Controller -Datapath Issues Under Investigation*

| Bug ID | Description |
|--------|--|
| 95532 | Symptom: A7210 controller running ArubaOS 6.3.1.1 stopped responding and rebooted. The log files for the event listed the reason as datapath timeout . |

Controller-Platform

Table 181: *Controller -Platform Issues Under Investigation*

| Bug ID | Description |
|--------|---|
| 95125 | Symptom: A controller unexpectedly reboots when upgrading to ArubaOS 6.3.0.2. |
| 102534 | Symptom: A 7240 controller running ArubaOS 6.4.0.3 crashed on kernel module. |
| 102930 | Symptom: A controller unexpectedly reboots with the reboot case: Soft Watchdog Reset. |
| 102534 | Symptom: A 7240 controller running ArubaOS 6.4.0.3 crashed on kernel module. |

This chapter details software upgrade procedures. Aruba best practices recommend that you schedule a maintenance window for upgrading your controllers.



Read all the information in this chapter before upgrading your controller.

Topics in this chapter include:

- [Upgrade Caveats on page 127](#)
- [Peer Controller Upgrade Requirement on page 128](#)
- [Installing the FIPS Version of ArubaOS 6.4.2.1 on page 128](#)
- [Important Points to Remember and Best Practices on page 129](#)
- [Memory Requirements on page 129](#)
- [Backing up Critical Data on page 130](#)
- [Upgrading in a Multi-Controller Network on page 131](#)
- [Upgrading to ArubaOS 6.4.2.1 on page 131](#)
- [Downgrading on page 135](#)
- [Before You Call Technical Support on page 137](#)

Upgrade Caveats

Before upgrading to this version of ArubaOS, take note of these known upgrade caveats.

- If your controller is running ArubaOS 6.4.0.0 or later versions, do not use Windows-based TFTP server to copy an ArubaOS image onto the non-boot partition of the controller for upgrading or downgrading. Use FTP or SCP to copy the image. For more information, see bug ID [97789 on page 110](#).
- AP LLDP profile is not supported on AP-120 Series in ArubaOS 6.4.x.
- Starting from ArubaOS 6.3.1.0, the local file upgrade option in the 620 and 650 controller WebUI has been disabled.
- The local file upgrade option in the 7200 Series controller WebUI does not work when upgrading from ArubaOS 6.2. When this option is used, the controller displays the error message **Content Length exceed limit** and the upgrade fails. All other upgrade options work as expected.
- ArubaOS 6.4.x does not allow you to create redundant firewall rules in a single ACL. ArubaOS will consider a rule redundant if the primary keys are the same. The primary key is made up of the following variables:
 - source IP/alias
 - destination IP/alias
 - proto-port/service

If you are upgrading from ArubaOS 6.1 or earlier and your configuration contains an ACL with redundant firewall rules, upon upgrading, only the last rule will remain.

For example, in the below ACL, both ACE entries could not be configured in ArubaOS 6.4.x. Once the second ACE entry is added, the first would be over written.

```
(host) (config) #ip access-list session allowall-laptop
(host) (config-sess-allowall-laptop)# any any any permit time-range test_range
(host) (config-sess-allowall-laptop)# any any any deny
(host) (config-sess-allowall-laptop)#end
(host) #show ip access-list allowall-laptop

ip access-list session allowall-laptop
allowall-laptop
-----
Priority Source Destination Service Action TimeRange
-----
1 any any any deny
```

- ArubaOS 6.4.x is supported only on the newer MIPS controllers (7200 Series, M3, 3200XM, 3400, 3600, and 600 Series). Legacy PPC controllers (200, 800, 2400, SC1/SC2) and 3200 controllers are not supported. Do not upgrade to ArubaOS 6.4.x if your deployment contains a mix of MIPS and PPC controllers in a master-local setup.
- When upgrading the software in a multi-controller network (one that uses two or more Aruba controllers), special care must be taken to upgrade all the controllers in the network and to upgrade them in the proper sequence. (See [Upgrading in a Multi-Controller Network on page 131](#).)
- PhoneHome setting will be disabled when the controller is upgraded from ArubaOS 6.4 to ArubaOS 6.4.0.1, regardless of whether PhoneHome was enabled or disabled. The current PhoneHome setting will be preserved if the controller is upgraded directly to ArubaOS 6.4.0.1 from ArubaOS 6.1, 6.2, or 6.3.

Peer Controller Upgrade Requirement

If you are running an L2 and L3 GRE tunnel between two or more Aruba controllers with **keepalive** enabled, all peer controllers must be upgraded to ArubaOS 6.4.1.0. This is not a requirement if **keepalive** is disabled on the peer controllers.



During the upgrade procedure, if one controller is upgraded and the other end point controller is yet to be upgraded, the GRE tunnel goes down. It is recommended to schedule a maintenance window to upgrade the peer controllers.

Points to Remember

- ArubaOS 6.4.1.0 continues to support L2 GRE tunnel type zero, but it is recommended to use a non-zero tunnel type.
- If both L2 and L3 tunnels are configured between end point devices, you must use a non-zero tunnel type for L2 GRE tunnels.

Installing the FIPS Version of ArubaOS 6.4.2.1

Download the FIPS version of the software from <https://support.arubanetworks.com>.

Before Installing FIPS Software

Before you install a FIPS version of software on a controller that is currently running a non-FIPS version of the software, you must reset the configuration to the factory default or you will not be able to login to the CLI or WebUI. Do this by running the **write erase** command just prior to rebooting the controller. This is the only supported method of moving from non-FIPS software to FIPS software.

Important Points to Remember and Best Practices

Ensure a successful upgrade and optimize your upgrade procedure by taking the recommended actions listed below. You should save this list for future use.

- Schedule the upgrade during a maintenance window and notify your community of the planned upgrade. This prevents users from being surprised by a brief wireless network outage during the upgrade.
- Avoid making any other changes to your network during the upgrade, such as configuration changes, hardware upgrades, or changes to the rest of the network. This simplifies troubleshooting.
- Know your network and verify the state of your network by answering the following questions.
 - How many APs are assigned to each controller? Verify this information by navigating to the **Monitoring > Network All Access Points** section of the WebUI, or by issuing the **show ap active** and **show ap database** CLI commands.
 - How are those APs discovering the controller (DNS, DHCP Option, Broadcast)?
 - What version of ArubaOS is currently on the controller?
 - Are all controllers in a master-local cluster running the same version of software?
 - Which services are used on the controllers (employee wireless, guest access, remote AP, wireless voice)?
- Resolve any existing issues (consistent or intermittent) before you upgrade.
- If possible, use FTP to load software images to the controller. FTP is faster than TFTP and offers more resilience over slow links. If you must use TFTP, ensure the TFTP server can send over 30 MB of data.
- Always upgrade the non-boot partition first. If problems occur during the upgrade, you can restore the flash, and switch back to the boot partition. Upgrading the non-boot partition gives you a smoother downgrade path should it be required.
- Before you upgrade to this version of ArubaOS, assess your software license requirements and load any new or expanded licenses you require. For a detailed description of these new license modules, refer to the “Software Licenses” chapter in the user guide.

Memory Requirements

All Aruba controllers store critical configuration data on an onboard compact flash memory module. Ensure that there is always free flash space on the controller. Loading multiple large files such as JPEG images for RF Plan can consume flash space quickly. To maintain the reliability of your WLAN network, the following compact memory best practices is recommended:

- Issue the **show memory** command to confirm that there is at least 40 MB of free memory available for an upgrade using the CLI, or at least 60 MB of free memory available for an upgrade using the WebUI. Do not proceed unless this much free memory is available. To recover memory, reboot the controller. After the controller comes up, upgrade immediately.
- Issue the **show storage** command to confirm that there is at least 60 MB of flash available for an upgrade using the CLI, or at least 75 MB of flash available for an upgrade using the WebUI.



In certain situations, a reboot or a shutdown could cause the controller to lose the information stored in its compact flash card. To avoid such issues, it is recommended that you issue the **halt** command before power cycling.

If the output of the **show storage** command indicates that insufficient flash memory space is available, you must free up additional memory. Any controller logs, crash data, or flash backups should be copied to a location off the controller, then deleted from the controller to free up flash space. You can delete the following files from the controller to free memory before upgrading:

- **Crash Data:** Issue the **tar crash** command to compress crash files to a file named **crash.tar**. Use the procedures described in [Backing up Critical Data on page 130](#) to copy the **crash.tar** file to an external server, then issue the command **tar clean crash** to delete the file from the controller.
- **Flash Backups:** Use the procedures described in [Backing up Critical Data on page 130](#) to back up the flash directory to a file named **flash.tar.gz**, then issue the command **tar clean flash** to delete the file from the controller.
- **Log files:** Issue the **tar logs** command to compress log files to a file named **logs.tar**. Use the procedures described in [Backing up Critical Data on page 130](#) to copy the **logs.tar** file to an external server, then issue the command **tar clean logs** to delete the file from the controller.

Backing up Critical Data

It is important to frequently backup all critical configuration data and files on the compact flash file system to an external server or mass storage device. At the very least, you should include the following files in these frequent backups:

- Configuration data
- WMS database
- Local user database
- Licensing database
- Floor plan JPEGs
- Custom captive portal pages
- x.509 certificates
- Controller Logs

Backup and Restore Compact Flash in the WebUI

The WebUI provides the easiest way to backup and restore the entire compact flash file system. The following steps describe how to backup and restore the compact flash file system using the WebUI on the controller:

1. Click on the **Configuration** tab.
2. Click **Save Configuration** at the top of the page.
3. Navigate to the **Maintenance > File > Backup Flash** page.
4. Click **Create Backup** to backup the contents of the compact flash file system to the **flashbackup.tar.gz** file.
5. Click **Copy Backup** to copy the file to an external server.
You can later copy the backup file from the external server to the compact flash file system using the file utility in the **Maintenance > File > Copy Files** page.
6. To restore the backup file to the Compact Flash file system, navigate to the **Maintenance > File > Restore Flash** page. Click **Restore**.

Backup and Restore Compact Flash in the CLI

The following steps describe the backup and restore procedure for the entire compact flash file system using the controller's command line:

1. Enter **enable** mode in the CLI on the controller, and enter the following command:
`(host) # write memory`
2. Use the backup command to backup the contents of the Compact Flash file system to the **flashbackup.tar.gz** file.
`(host) # backup flash`
Please wait while we tar relevant files from flash...

```
Please wait while we compress the tar file...
Checking for free space on flash...
Copying file to flash...
File flashback.tar.gz created successfully on flash.
```

3. Use the copy command to transfer the backup flash file to an external server or storage device:

```
(host) copy flash: flashback.tar.gz ftp: <ftphost> <ftpusername> <ftpuserpassword>
<remote directory>
(host) copy flash: flashback.tar.gz usb: partition <partition-number>
```

You can later transfer the backup flash file from the external server or storage device to the Compact Flash file system with the copy command:

```
(host) # copy tftp: <tftphost> <filename> flash: flashback.tar.gz
(host) # copy usb: partition <partition-number> <filename> flash: flashback.tar.gz
```

4. Use the restore command to untar and extract the **flashbackup.tar.gz** file to the compact flash file system:

```
(host) # restore flash
```

Upgrading in a Multi-Controller Network

In a multi-controller network (a network with two or more Aruba controllers), special care must be taken to upgrade all controllers based on the controller type (master or local). Be sure to back up all controllers being upgraded, as described in [Backing up Critical Data on page 130](#).



For proper operation, all controllers in the network must be upgraded with the same version of ArubaOS software. For redundant (VRRP) environments, the controllers should be the same model.

To upgrade an existing multi-controller system to this version of ArubaOS:

1. Load the software image onto all controllers (including redundant master controllers).
2. If all the controllers cannot be upgraded with the same software image and rebooted simultaneously, use the following guidelines:
 - a. Upgrade the software image on all the controllers. Reboot the master controller. Once the master controller completes rebooting, you can reboot the local controllers simultaneously.
 - b. Verify that the master and all local controllers are upgraded properly.

Upgrading to ArubaOS 6.4.2.1

Install Using the WebUI



Confirm that there is at least 60 MB of free memory and at least 75 MB of flash available for an upgrade using the WebUI. For details, see [Memory Requirements on page 129](#)



When you navigate to the **Configuration** tab of the controller's WebUI, the controller may display an error message **Error getting information: command is not supported on this platform**. This error occurs when you upgrade the controller from the WebUI and navigate to the **Configuration** tab as soon as the controller completes rebooting. This error is expected and disappears after clearing the web browser cache.

Upgrading From an Older version of ArubaOS

Before you begin, verify the version of ArubaOS currently running on your controller. If you are running one of the following versions of ArubaOS, you must download and upgrade to an interim version of ArubaOS before upgrading to ArubaOS 6.4.2.1.

- For ArubaOS 3.x.versions earlier than ArubaOS 3.4.4.1, download the latest version of ArubaOS 3.4.5.x.

- For ArubaOS 3.x or ArubaOS 5.0.x versions earlier than ArubaOS 5.0.3.1, download and install the latest version of ArubaOS 5.0.4.x.
- For ArubaOS 6.0.0.0 or 6.0.0.1 versions, download and install the latest version of ArubaOS 6.0.1.x.

Follow step 2 to step 11 of the procedure described in [Upgrading From a Recent version of ArubaOS on page 132](#) to install the interim version of ArubaOS, then repeat step 1 to step 11 of the procedure to download and install ArubaOS 6.4.2.1.

Upgrading From a Recent version of ArubaOS

The following steps describe the procedure to upgrade from one of the following recent versions of ArubaOS:

- 3.4.4.1 or later
- 5.0.3.1 or later 5.0.x (If you are running ArubaOS 5.0.3.1 or the latest 5.0.x.x, review [Upgrading to ArubaOS 6.4.2.1 on page 131](#) before proceeding further.)
- 6.0.1.0 or later 6.x

Install the ArubaOS software image from a PC or workstation using the Web User Interface (WebUI) on the controller. You can also install the software image from a TFTP or FTP server using the same WebUI page.

1. Download ArubaOS 6.4.2.1 from the customer support site.
2. Upload the new software image(s) to a PC or workstation on your network.
3. Validate the SHA hash for a software image:
 - a. Download the file **Aruba.sha256** from the download directory.
 - b. To verify the image, load the image onto a Linux system and execute the command **sha256sum <filename>** or use a suitable tool for your operating system that can generate a **SHA256** hash of a file.
 - c. Verify that the output produced by this command matches the hash value found on the support site.



The ArubaOS image file is digitally signed, and is verified using RSA2048 certificates pre-loaded on the controller at the factory. Therefore, even if you do not manually verify the SHA hash of a software image, the controller will not load a corrupted image.

4. Log in to the ArubaOS WebUI from the PC or workstation.
5. Navigate to the **Maintenance > Controller > Image Management** page.
 - a. Select the **Upload Local File** option.
 - b. Click **Browse** to navigate to the saved image file on your PC or workstation.
6. Select the downloaded image file.
7. In the **partition to upgrade** field, select the non-boot partition.
8. In the **Reboot Controller After Upgrade** option field, best practices is to select **Yes** to automatically reboot after upgrading. If you do not want the controller to reboot immediately, select **No**.



Note however, that the upgrade will not take effect until you reboot the controller.

9. In the **Save Current Configuration Before Reboot** field, select **Yes**.
10. Click **Upgrade**.

When the software image is uploaded to the controller, a popup window displays the message **Changes were written to flash successfully**.
11. Click **OK**.

If you chose to automatically reboot the controller in step 8, the reboot process starts automatically within a few seconds (unless you cancel it).

12. When the reboot process is complete, log in to the WebUI and navigate to the **Monitoring > Controller > Controller Summary** page to verify the upgrade.

Once your upgrade is complete, perform the following steps to verify that the controller is behaving as expected.

1. Log in into the WebUI to verify all your controllers are up after the reboot.
2. Navigate to **Monitoring > Network Summary** to determine if your APs are up and ready to accept clients.
3. Verify that the number of access points and clients are what you would expect.
4. Test a different type of client for each access method that you use and in different locations when possible.
5. Complete a back up of all critical configuration data and files on the compact flash file system to an external server or mass storage facility. See [Backing up Critical Data on page 130](#) for information on creating a backup. If the flash (Provisioning/Backup) image version string shows the letters *rn*, for example, 3.3.2.11-rn-3.0, note those AP names and IP addresses. The RAP-5/RAP-5WN reboots to complete the provisioning image upgrade.

Install Using the CLI



Confirm that there is at least 40 MB of free memory and at least 60 MB of flash available for an upgrade using the CLI. For details, see [Memory Requirements on page 129](#).

Upgrading From an Older Version of ArubaOS

Before you begin, verify the version of ArubaOS currently running on your controller. If you are running one of the following versions of ArubaOS, you must download and upgrade to an interim version of ArubaOS before upgrading to ArubaOS 6.4.2.1.

- For ArubaOS 3.x versions earlier than ArubaOS 3.4.4.1, download the latest version of ArubaOS 3.4.5.x.
- For ArubaOS RN-3.x or ArubaOS 5.0.x versions earlier than ArubaOS 5.0.3.1, download the latest version of ArubaOS 5.0.4.x.
- For ArubaOS 6.0.0.0 or 6.0.0.1 versions, download the latest version of ArubaOS 6.0.1.x.

Follow step 2 - step 7 of the procedure described in [Upgrading From a Recent Version of ArubaOS on page 133](#) to install the interim version of ArubaOS, then repeat step 1 to step 7 of the procedure to download and install ArubaOS 6.4.2.1.

Upgrading From a Recent Version of ArubaOS

The following steps describe the procedure to upgrade from one of the following recent versions of ArubaOS:

- 3.4.4.1 or later
- 5.0.3.1 or later 5.0.x (If you are running ArubaOS 5.0.3.1 or the latest 5.0.x.x, review [Upgrading to ArubaOS 6.4.2.1 on page 131](#) before proceeding further.)
- 6.0.1.0 or later 6.x

To install the ArubaOS software image from a PC or workstation using the Command-Line Interface (CLI) on the controller:

1. Download ArubaOS 6.4.2.1 from the customer support site.
2. Open a Secure Shell session (SSH) on your master (and local) controllers.
3. Execute the **ping** command to verify the network connection from the target controller to the SCP/FTP/TFTP server:

```
(hostname) # ping <ftphost>
```

or

```
(hostname)# ping <tftphost>
```

or

```
(hostname)# ping <scphost>
```

4. Use the **show image version** command to check the ArubaOS images loaded on the controller's flash partitions. The partition number appears in the **Partition** row; **0:0** is partition 0, and **0:1** is partition 1. The active boot partition is marked as **Default boot**.

```
(hostname)# show image version
```

```
-----  
Partition           : 0:0 (/dev/hal)  
Software Version    : ArubaOS 6.1.1.0 (Digitally Signed - Production Build)  
Build number        : 28288  
Label               : 28288  
Built on            : Thu Apr 21 12:09:15 PDT 2012  
-----  
Partition           : 0:1 (/dev/hda2) **Default boot**  
Software Version    : ArubaOS 6.1.3.2 (Digitally Signed - Production Build)  
Build number        : 38319  
Label               : 38319  
Built on            : Fri June 07 00:03:14 2013
```

5. Use the **copy** command to load the new image onto the non-boot partition:

```
(hostname)# copy ftp: <ftphost> <ftpusername> <image filename> system: partition <0|1>
```

or

```
(hostname)# copy tftp: <tftphost> <image filename> system: partition <0|1>
```

or

```
(hostname)# copy scp: <scphost> <scpusername> <image filename> system: partition <0|1>
```

or

```
(hostname)# copy usb: partition <partition-number> <image filename> system: partition <0|1>
```



The USB option is only available on the 7200 Series controllers.

6. Issue the **show image version** command to verify the new image is loaded:

```
(hostname)# show image version
```

```
-----  
Partition           : 0:0 (/dev/hda1) **Default boot**  
Software Version    : ArubaOS 6.4.2.1 (Digitally Signed - Beta Build)  
Build number        : 46040  
Label               : 46040  
Built on            : Thu Sep 18 10:52:27 PDT 2014  
-----  
Partition           : 0:1 (/dev/hda2)  
Software Version    : ArubaOS 6.1.3.2 (Digitally Signed - Production Build)  
Build number        : 38319  
Label               : 38319  
Built on            : Fri June 07 00:03:14 2013
```

7. Reboot the controller:

```
(hostname)# reload
```

8. Execute the **show version** command to verify the upgrade is complete.

```
(hostname)# show version
```

Once your upgrade is complete, perform the following steps to verify that the controller is behaving as expected.

1. Log in into the command-line interface to verify all your controllers are up after the reboot.
2. Issue the **show ap active** command to determine if your APs are up and ready to accept clients.
3. Issue the **show ap database** command to verify that the number of access points and clients are what you expected.
4. Test a different type of client for each access method that you use and in different locations when possible.
5. Complete a backup of all critical configuration data and files on the compact flash file system to an external server or mass storage facility. See [Backing up Critical Data on page 130](#) for information on creating a backup.

Downgrading

If necessary, you can return to your previous version of ArubaOS.



If you upgraded from 3.3.x to 5.0, the upgrade script encrypts the internal database. New entries created in ArubaOS 6.4.2.1 are lost after the downgrade (this warning does not apply to upgrades from 3.4.x to 6.1).



If you do not downgrade to a previously-saved pre-6.1 configuration, some parts of your deployment may not work as they previously did. For example, when downgrading from ArubaOS 6.4.2.1 to 5.0.3.2, changes made to WIPS in 6.x prevents the new predefined IDS profile assigned to an AP group from being recognized by the older version of ArubaOS. This unrecognized profile can prevent associated APs from coming up, and can trigger a profile error.

These new IDS profiles begin with **ids-transitional** while older IDS profiles do not include transitional. If you have encountered this issue, use the **show profile-errors** and **show ap-group** commands to view the IDS profile associated with AP Group.



When reverting the controller software, whenever possible, use the previous version of software known to be used on the system. Loading a release not previously confirmed to operate in your environment could result in an improper configuration.

Before You Begin

Before you reboot the controller with the pre-upgrade software version, you must perform the following steps:

1. Back up your controller. For details, see [Backing up Critical Data on page 130](#).
2. Verify that control plane security is disabled.
3. Set the controller to boot with the previously-saved pre-ArubaOS 6.4.2.1 configuration file.
4. Set the controller to boot from the system partition that contains the previously running ArubaOS image.

When you specify a boot partition (or copy an image file to a system partition), the software checks to ensure that the image is compatible with the configuration file used on the next controller reload. An error message displays if system boot parameters are set for incompatible image and configuration files.

5. After downgrading the software on the controller:
 - Restore pre-ArubaOS 6.4.2.1 flash backup from the file stored on the controller. Do not restore the ArubaOS 6.4.2.1 flash backup file.
 - You do not need to re-import the WMS database or RF Plan data. However, if you have added changes to RF Plan in ArubaOS 6.4.2.1, the changes do not appear in RF Plan in the downgraded ArubaOS version.
 - If you installed any certificates while running ArubaOS 6.4.2.1, you need to reinstall the certificates in the downgraded ArubaOS version.

Downgrading Using the WebUI

The following sections describe how to use the WebUI to downgrade the software on the controller.

1. If the saved pre-upgrade configuration file is on an external FTP/TFTP server, copy the file to the controller by navigating to the **Maintenance > File > Copy Files** page.
 - a. For **Source Selection**, select FTP/TFTP server, and enter the IP address of the FTP/TFTP server and the name of the pre-upgrade configuration file.
 - b. For **Destination Selection**, enter a filename (other than default.cfg) for Flash File System.
2. Set the controller to boot with your pre-upgrade configuration file by navigating to the **Maintenance > Controller > Boot Parameters** page.
 - a. Select the saved pre-upgrade configuration file from the Configuration File menu.
 - b. Click **Apply**.
3. Determine the partition on which your previous software image is stored by navigating to the **Maintenance > Controller > Image Management** page. If there is no previous software image stored on your system partition, load it into the backup system partition (you cannot load a new image into the active system partition):
 - a. Enter the FTP/TFTP server address and image file name.
 - b. Select the backup system partition.
 - c. Click **Upgrade**.
4. Navigate to the **Maintenance > Controller > Boot Parameters** page.
 - a. Select the system partition that contains the pre-upgrade image file as the boot partition.
 - b. Click **Apply**.
5. Navigate to the **Maintenance > Controller > Reboot Controller** page. Click **Continue**. The controller reboots after the countdown period.
6. When the boot process is complete, verify that the controller is using the correct software by navigating to the **Maintenance > Controller > Image Management** page.

Downgrading Using the CLI

The following sections describe how to use the CLI to downgrade the software on the controller.

1. If the saved pre-upgrade configuration file is on an external FTP/TFTP server, use the following command to copy it to the controller:

```
(host) # copy ftp: <ftphost> <ftpusername> <image filename> system: partition 1
```

or

```
(host) # copy tftp: <tftphost> <image filename> system: partition 1
```

2. Set the controller to boot with your pre-upgrade configuration file.

```
(host) # boot config-file <backup configuration filename>
```

3. Execute the **show image version** command to view the partition on which your previous software image is stored. You cannot load a new image into the active system partition (the default boot).

In the following example, partition 1, the backup system partition, contains the backup release ArubaOS 6.1.3.2. Partition 0, the default boot partition, contains the ArubaOS 6.4.2.1 image:

```
#show image version
```

```
-----  
Partition           : 0:0 (/dev/hda1) **Default boot**  
Software Version    : ArubaOS 6.4.2.1 (Digitally Signed - Beta Build)  
Build number        : 46040  
Label               : 46040  
Built on            : Thu Sep 18 10:52:27 PDT 2014  
-----  
Partition           : 0:1 (/dev/hda2)
```



```
Software Version      : ArubaOS 6.1.3.2 (Digitally Signed - Production Build)
Build number         : 38319
Label                : 38319
Built on             : Fri June 07 00:03:14 2013
```

4. Set the backup system partition as the new boot partition:

```
(host) # boot system partition 1
```

5. Reboot the controller:

```
(host) # reload
```

6. When the boot process is complete, verify that the controller is using the correct software:

```
(host) # show image version
```

Before You Call Technical Support

Before you place a call to Technical Support, follow these steps:

1. Provide a detailed network topology (including all the devices in the network between the user and the Aruba controller with IP addresses and Interface numbers if possible).
2. Provide the wireless device's make and model number, OS version (including any service packs or patches), wireless NIC make and model number, wireless NIC's driver date and version, and the wireless NIC's configuration.
3. Provide the controller logs and output of the **show tech-support** command via the WebUI Maintenance tab or via the CLI (**tar logs tech-support**).
4. Provide the syslog file of the controller at the time of the problem. Aruba strongly recommends that you consider adding a syslog server if you do not already have one to capture logs from the controller.
5. Let the support person know if this is a new or existing installation. This helps the support team to determine the troubleshooting approach, depending on whether you have an outage in a network that worked in the past, a network configuration that has never worked, or a brand new installation.
6. Let the support person know if there are any recent changes in your network (external to the Aruba controller) or any recent changes to your controller and/or AP configuration. If there was a configuration change, list the exact configuration steps and commands used.
7. Provide the date and time (if possible) when the problem first occurred. If the problem is reproducible, list the exact steps taken to recreate the problem.
8. Provide any wired or wireless sniffer traces taken during the time of the problem.
9. Provide the controller site access information, if possible.

